Contract # **MA262-1**

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Division of Purchasing and the following Contractor:

Sprint Solutions, Inc.
Name
12502 Sunrise Valley Drive, Mailstop: VARESA0208
Address
Reston Virginia 20196
City State Zip

LEGAL STATUS OF CONTRACTOR
□ Sole Proprietor
□ Non-Profit Corporation
☒ For-Profit Corporation
□ Partnership
□ Government Agency

Contact Person Shannon Hewitt-Tapp Phone 916-275-3146 Email Shannon.Hewitt-Tapp@sprint.com
Vendor #VC0000108646 Commodity Code #72551, 91579

2. GENERAL PURPOSE OF CONTRACT: The general purpose of this contract is to provide: Wireless Data, Voice & Accessories.

3. PROCUREMENT: This contract is entered into as a result of the procurement process on Bid# CJ18012.

4. CONTRACT PERIOD: Effective Date: 12/6/2019 Termination Date: 8/11/2024 unless terminated early or extended in accordance with the terms and conditions of this contract. Renewal options (if any): Contract may be extended an additional 5 years.

5. Payment: Prompt Payment Discount (if any): N/A.

6. Administrative Fee, as described in the Solicitation and Attachment A: Section 6 0.25% on Corporate/Government Responsible (CRU)/ 0.10% on all Individual Responsible (IRU).

7. ATTACHMENT A: NASPO ValuePoint Master Agreement Terms and Conditions for ☒ Goods ☒ Services, or □ IT
ATTACHMENT AA: Contractors Supplemental Terms and Conditions
ATTACHMENT B: Scope of Work
ATTACHMENT C: Cost Sheet
ATTACHMENT G: Plan Description
ATTACHMENT H: Award Category 1 Reporting Template
ATTACHMENT I: Award Category 2 Reporting Template
ATTACHMENT J: Award Category 3 Reporting Template
ATTACHMENT L: Network Technology Questionnaire
ATTACHMENT M: New Product Request Form
ATTACHMENT N: New Product Log
ATTACHMENT S: Security Disclosures
ATTACHMENT V: Award Category Sheet
ATTACHMENT W: Award Category Sheet

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah State Procurement Code, Procurement Rules, Contractor's response to Bid # CJ18012, and the Solicitation #CJ18012.

9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Kimberly Green-Kerr 12/10/2019
Contractor's signature Date
Kimberly Green-Kerr, Senior Vice President – Sprint Business Solutions
Type or Print Name and Title

STATE

Dec 11, 2019
Director, Division of Purchasing Date

Sprint Approved as to Legal Form
TFD
06 Dec 2019

APPROVED
P&CA
AB
12/10/2019

Christopher Jennings	801-538-3157	N/A	ctjennings@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

Attachment A:
NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum ("PA");
(2) NASPO ValuePoint Master Agreement Terms and Conditions;
(3) A Purchase Order issued against the Master Agreement;
(5) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State including Attachment AA Contractor's Additional Terms and Conditions
(6) The Solicitation or, if separately executed after award, the Lead State's bilateral agreement that integrates applicable provisions.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions

Acceptance is defined by the applicable State commercial code, except Acceptance shall not occur before the completion of delivery in accordance with the Order, installation if required, and a reasonable time for inspection of the Product in accordance with Section 15 of this Master Agreement. This definition is not intended to limit rights and remedies under applicable State law.

Contractor means the person or entity delivering Products or performing services under the terms and conditions set forth in this Master Agreement.

Embedded Software means one or more software applications which permanently reside on a computing device.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering any resulting Master Agreement(s).

Master Agreement means the underlying agreement executed by and between the Lead State, acting on behalf of the NASPO ValuePoint program, and the Contractor, as now or hereafter amended.

NASPO ValuePoint is the cooperative contracting arm of the National Association of State Procurement Officials (NASPO) a non-profit organization formed in 1947 to promote public procurement throughout the country. NASPO ValuePoint facilitates administration of the NASPO cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states, the District of Columbia, and territories of the United States. NASPO ValuePoint is identified in the Master Agreement as the recipient of reports and the NASPO ValuePoint administrative fee; and may perform contract administration functions relating to collecting and receiving reports and fees, as well as other contract administration functions as assigned by the Lead State.

Order or **Purchase Order** means any purchase order, sales order, contract or other document used by a Purchasing Entity to order the Products and Services.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions, etc.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity; however, a Participating State listed in the Request for Proposal is not required to participate through execution of a Participating Addendum.

Product means any equipment, software (including embedded software), documentation, hardware, cabling, other materials sold or leased to Purchasing Entity, service, or other deliverable supplied by the Contractor pursuant to this Master Agreement. The term Products, supplies and services, and products and services are used interchangeably in these terms and conditions, except where the sense and context are intended to distinguish between products and services.

Purchasing Entity means a state (as well as the District of Columbia and U.S territories), city, county, district, other political subdivision of a State, or a nonprofit organization under the laws of some states if authorized by a Participating Addendum that issues a Purchase Order against the Master Agreement.

Services mean wireless service plans and related installation and maintenance services or other solutions.

Additional definitions are set forth in Attachment AA, Contractor's Additional Terms and Conditions.

NASPO ValuePoint Program Provisions

3. Term of the Master Agreement

a. The initial term of this Master Agreement is set forth in the State of Utah Cooperative Contract, Section 4 Contract Period. This Master Agreement may be extended beyond the original contract period for up to Five (5) additional years at the Lead State's discretion and by mutual written agreement of Contractor and upon review of requirements of Participating Entities, current market conditions, and Contractor performance.

b. The Master Agreement may, subject to the mutual written agreement of the Contractor and the Lead State, be extended for a reasonable period of time in adherence to the Lead State's Procurement Code, if in the judgment of the Lead State a follow-on, competitive procurement will be unavoidably delayed (despite good faith efforts) beyond the planned date of execution of the follow-on master agreement. This subsection shall not be deemed to limit the authority of a Lead State under its state law otherwise to negotiate contract extensions.

4. Amendments

The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written agreement of the Lead State and Contractor.

5. Participants and Scope

a. Contractor may not deliver Products under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed Additional methods of ordering may be utilized if agreed to in writing by the Lead State, NASPO, and the Contractor. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Purchasing Entity, except to the extent altered, modified, supplemented or amended by a Participating Addendum (or included in a Purchase Order, as expressly required by a Purchasing Entity's laws or regulations). By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts are subject to the approval of the respective State Chief Procurement Official. Issues of interpretation and eligibility for participation are solely within the authority of the respective State Chief Procurement Official.

c. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of

Participating Entities who are states are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating Entities who are states incur no financial obligations on behalf of other Purchasing Entities. Contractor shall email a fully executed PDF copy of each Participating Addendum to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

d. NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint, and NASPO (National Association of State Procurement Officials) are not a party to the Master Agreement. NASPO/NASPO ValuePoint is a nonprofit cooperative purchasing organization assisting states in administering the NASPO cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

e. Participating Addenda shall not be construed to amend the following provisions in this Master Agreement between the Lead State and Contractor that prescribe NASPO ValuePoint Program requirements: Term of the Master Agreement; Amendments; Participants and Scope; Administrative Fee; NASPO ValuePoint Summary and Detailed Usage Reports; NASPO ValuePoint Cooperative Program Marketing and Performance Review; Right to Publish; Price and Rate Guarantee Period; and Individual Customers. Any such language shall be void and of no effect.

f. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the consent to participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum or placement of a Purchase Order, pursuant to Section 5a above, is not a determination that procurement authority exists in the Participating Entity; each entity must ensure that they have the requisite procurement authority to execute a Participating Addendum or place an Order under the Master Agreement.

g. Resale. “Resale” means any payment in exchange for transfer of tangible goods, software, or assignment of the right to services. Subject to any specific conditions included in the solicitation agreed to by the Contractor or Contractor’s proposal as accepted by the Lead State, or as explicitly permitted in a Participating Addendum, Purchasing Entities may not resell Products or Services. Absent any such condition or explicit permission, this limitation does not prohibit reselling of Unsubsidized Devices that have been paid for in full by Purchasing Entity or Subsidized Devices that have fulfilled the applicable Minimum Service Term, in the following limited scenarios: (1) transfers between public agencies; (2) sales in accordance with an entity’s surplus property laws; and (3) fees associated with inventory transactions with other governmental or nonprofit entities and consistent with a Purchasing Entity’s laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

6. Administrative Fees

a. The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of 0.25% on Corporate/Government Responsible (CRU) accounts and 0.10% on all Individual Responsible (IRU) accounts no later than sixty (60) days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on all sales of Products and Services for both Corporate/Government Responsible (CRU) and Individual Response (IRU) accounts under the Master Agreement (less any charges for taxes, applicable surcharges, regulatory fees, credits, refunds or shipping). The

NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with the proposal. Contractor's obligation to pay the NASPO ValuePoint Administrative Fee terminates if: (1) the Master Agreement has expired; or (2) the Master Agreement has been terminated (before expiration) by either party. Contractor shall pay in accordance with this Section 6a. the NASPO ValuePoint Administrative Fee on all sales or products and services through the effective date of expiration or termination of the Master Agreement.

b. Additionally, some states may require an additional fee be paid directly to the state only on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee in subsection 6a shall be based on the gross amount of all sales (less any charges for taxes, applicable surcharges, regulatory fees, credits, refunds or shipping) at the adjusted prices (if any) in Participating Addenda. Unless otherwise set forth in a Participating Addendum, Contractor's obligation to pay a Participating State an additional fee on purchases made by Purchasing Entities within that State terminates if: (1) the Participating Addendum for that Participating State has expired; or (2) the Participating Addendum for that Participating State has been terminated (before expiration) by either party. Contractor shall pay a Participating State in accordance with this Section 6b the additional fee on all sales of Products and Service through the effective date of expiration or termination of the applicable Participating Addendum.

7. NASPO ValuePoint Summary and Detailed Usage Reports

In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org, or as otherwise agreed to by the Parties in writing. Any/all sales made under this Master Agreement shall be reported as cumulative totals by state for Government Responsible accounts. A separate report shall be submitted and reported as cumulative totals by state for Individual Responsible (IRU) accounts. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than forty-five (45) days following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data using the format provided in Attachments H, I, J and K. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint no later than forty-five (45) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint electronically through a designated portal, email, CD-ROM, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement.

c. Reportable sales for the summary sales data report and detailed sales data report includes aggregated sales to employees on IRU Accounts for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, **social security numbers, or any other numerical identifier considered Personally Identifiable Information**, may be submitted with any report.

d. Contractor shall provide NASPO ValuePoint with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any Participating Addendum roll out or implementation activities and issues. NASPO ValuePoint and Contractor will determine the format and content of the executive summary. The executive summary is due forty-five (45) days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. NASPO and Contractor acknowledge and agree that Contractor is under a duty to adhere to all applicable Federal Law, including but not limited to 47 U.S.C § 201(b) and 222, that require protection of information regarding Contractor's customers.

8. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master Agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel, to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the Participating Addendum. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, cancel the Master Agreement pursuant to section 27, or not exercise an option to renew, when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. Cancellation based on nonuse or under-utilization will not occur sooner than one year after award (or execution if later) of the Master Agreement. This subsection does not limit the discretionary right of either the Lead State or Contractor to cancel the Master Agreement pursuant to section 27 or to terminate for default pursuant to section 29.

g. Contractor shall notify the Lead State and NASPO ValuePoint of any contractual most- favored-customer provisions in any Cooperative Purchasing Agreements with a like government member eligibility that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this Master Agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions. For the purposes of this paragraph, Cooperative Purchasing Agreement shall mean a cooperative purchasing program facilitating public procurement solicitations and agreements using a lead- agency model. This does not include contracts with any federal agency or any federal contract, or any state agency or any state contract.

9. Right to Publish

Throughout the duration of this Master Agreement, Contractor must secure from the Lead State prior approval for the release of information that pertains to the potential work or activities covered by the Master Agreement. This limitation does not preclude publication about the award of the Master Agreement or marketing activities consistent with any proposed and accepted marketing plan. The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the Products or Services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Price and Rate Adjustment

Contractor shall not charge a Purchasing Entity or individual a price higher than that set forth in this Master Agreement. Requests for price or rate adjustment increases must a) include sufficient documentation supporting the request; and b) be reflected in a written amendment to this Master Agreement. Any adjustment or amendment to the Master Agreement shall not be effective unless approved in writing by the Lead State and executed by the Parties. No retroactive adjustments to prices or rates will be allowed. Notwithstanding the foregoing, any new Products or Services offered by Contractor shall not be deemed a price or rate adjustment under this Section 10.

11. Individual Customers

Except to the extent modified by a Participating Addendum or Purchase Order, pursuant to Section 5, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

Administration of Orders

12. Ordering

a. Upon request from the Purchasing Entity, the Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. Purchasing Entities may define entity or project-specific requirements and informally compete the requirement among companies having a Master Agreement on an “as needed” basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to the Purchasing Entity’s rules and policies. The Purchasing Entity may in its sole discretion determine which Master Agreement Contractors should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

Notwithstanding the foregoing, discounts or promotional prices may be offered at any time and do not need the approval of NASPO or the Purchasing Entity. An informal solicitation pursuant to the terms of the Master Agreement does not need to be issued by the Purchasing Entity to receive discounts and promotional prices. The prices listed in the Master Agreement are ceiling prices and therefore any discounts or promotional prices offered cannot exceed the price listed in the Master Agreement.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities’ rules, policies, and procedures regarding the ordering of Products and/or Services contemplated by this Master Agreement.

d. Contractor shall not begin work without a valid Purchase Order or other appropriate commitment or funding document under the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per hour or other pricing elements consistent with this Master Agreement and the contractor’s proposal;
(6) The estimated amount of the Order, not including any government taxes, fees or surcharges and additional service charges (if applicable); and
(7) The Master Agreement identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity’s purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date thereof, but may have a delivery date or performance period up to 120 days past the then-current termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration, cancellation or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration, cancellation or termination of this Master Agreement, or otherwise inconsistent with its terms. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

13. Shipping and Delivery

a. The prices are the delivered price to any Purchasing Entity. All deliveries shall be F.O.B. destination, freight pre-paid, with all standard transportation and handling charges paid by the Contractor. Additional charges will apply for overnight or expedited shipping initiated by the Purchasing Entity. Responsibility and liability for loss or damage shall remain the Contractor's until final inspection and acceptance when responsibility shall pass to the Purchasing Entity except as to latent defects, fraud, and Contractor's warranty obligations (if any). The minimum shipment amount, if any, will be found in the special terms and conditions. Any order for less than the specified amount is to be shipped with the freight prepaid and added as a separate item on the invoice. Any portion of an Order to be shipped without transportation charges that is back ordered shall be shipped via standard shipping without charges.

b. Only upon request and as specifically designated in an order form or Purchase Order by a representative of the Purchasing Entity placing the Order, Contractor shall provide for Inside Delivery. "Inside Delivery" refers to a delivery to other than a loading dock, front lobby, or reception area. For any Inside Delivery agreed to by Contractor, any damage to the building interior, scratched walls, damage to the freight elevator, etc., will be the responsibility of the Contractor. If damage does occur, it is the responsibility of the Contractor to immediately notify the Purchasing Entity placing the Order.

c. All products must be delivered in the manufacturer's standard package. Costs shall include' packing and/or crating charges. Cases shall be of durable construction, good condition, properly labeled and suitable in every respect for storage and handling of contents. Upon request by the Purchasing Entity, each shipping carton shall be marked with the Purchasing Entity's Purchase Order number.

14. Laws and Regulations

Any and all Products and Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

15. Inspection and Acceptance

a. Where the Master Agreement or an Order does not otherwise specify a process for inspection and Acceptance, this section governs. This section is not intended to limit rights and remedies under the applicable commercial code.

b. All Products are subject to inspection at reasonable times and places before Acceptance. Contractor shall provide right of access to the Lead State, or to any other authorized agent or official of the Lead State or other Participating or Purchasing Entity, at reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance requirements under this Master Agreement. Shipment of Products that do not visibly meet specifications when received by a Purchasing Entity may be rejected as nonconforming. Failure to reject upon receipt, however, does not relieve the Contractor of liability for material (nonconformity that substantial impairs value) latent or hidden defects subsequently revealed when goods are put to use. Acceptance of such goods may be revoked in accordance with this Section 15. The Contractor is liable for any resulting commercially reasonable expense incurred by the Purchasing Entity related to the preparation and standard ground transportation shipping charges associated with the nonconforming Products rejected and returned, or for which Acceptance is revoked. Nonconforming Products rejected and returned shall be in accordance with the Acceptance Testing period as described in Section 5e below.

c. If any Service(s) do not conform to contract requirements, the Purchasing Entity may require the Contractor to perform the services again in conformity with contract requirements, at no increase in Order amount. When defects cannot be corrected by re-performance, the Purchasing Entity may require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and reduce the contract price, upon mutual agreement of the Parties, to reflect the reduced value of Services performed.

d. INTENTIONALLY OMITTED

e. Acceptance Testing may be explicitly set out in an Order to ensure conformance to an explicit standard of performance. Acceptance Testing means the process set forth in an Order for ascertaining that the Product or Service meets the standard of performance prior to Acceptance by the Purchasing Entity. If Acceptance Testing is prescribed, this subsection applies to applicable Products or Services purchased under this Master Agreement, including any additional, replacement, or substitute Product(s) or Service(s) and any Product(s) or Service(s) which are modified by or with the written approval of Contractor after Acceptance by the Purchasing Entity. The Acceptance Testing period shall be sixty (60) calendar days, or other time period identified in a Participating Addendum, starting from the day the Product and/or Service is activated (or of purchase if the Product is delivered without activating service) or, if installed, the day the Product or Service is installed and Contractor advises that the Product or Service is ready for Acceptance Testing. If the Product does not meet the standard of performance during the Acceptance Testing period, Purchasing Entity may return the nonconforming Products in the same condition received by the Purchasing Entity to the original place of purchase. Purchasing Entity must contact Contractor to deactivate Service prior to the end of the Acceptance Testing period. If Purchasing Entity does not return the nonconforming Product or deactivate the Service prior to the end of the Acceptance Testing period, the Purchasing Entity will be deemed to have accepted the Product(s) and/or Service(s). Contractor shall pay all commercially reasonable costs related to the preparation and standard ground transportation shipping costs associated with the nonconforming Product or Service returned pursuant to this section. The warranty period shall begin as outlined in the manufacturer's warranty provided directly from the manufacturer as described in the Warranty section of this Master Agreement.

16. Payment

Payment to Contractor is required within 30 days following the date the entire order is delivered or the date a correct invoice is received, whichever is later. After 45 days, the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance, unless a different late payment amount is specified in a Participating Addendum, Order, or otherwise prescribed by applicable law. Payments will be remitted by mail or electronic funds transfer (EFT). Payments may be made via a State or political subdivision “Purchasing Card” with no additional charge.

17. Warranty

a. General Warranty. Contractor will perform all Services in a good and workmanlike manner consistent with accepted industry practice and in compliance with applicable laws and regulations. To the maximum extent possible, Contractor will pass through to Purchasing Entities all warranties available to Contractor for any Product(s) acquired hereunder.

b. The Contractor warrants that the Product shall be delivered new and in original manufacturer’s packaging, except where Purchasing Entity and Contractor otherwise agree to utilize refurbished Products. Because the Contractor is not the manufacturer of the Product, it provides the Product “as-is” and agrees to pass through the standard device manufacturer warranty (generally, 12 months) to the Purchasing Entity. The rights and remedies of the parties under this warranty are in addition to any other rights and remedies of the parties provided by law or equity. Except as provided in this Section 17, Contractor disclaims all express or implied warranties.

18. Title of Product

Upon Acceptance by the Purchasing Entity, Contractor shall convey to Purchasing Entity title to the Product free and clear of all liens, encumbrances, or other security interests. Transfer of title to the Product shall include an irrevocable and perpetual license to use any Embedded Software in the Product, subject to any applicable license provisions or acceptable use policies. If Purchasing Entity subsequently transfers title of the Product to another entity, Purchasing Entity shall have the right to transfer the license to use the Embedded Software with the transfer of Product title, subject to any license provisions or acceptable use policies related to any Embedded Software. A subsequent transfer of this software license shall be at no additional cost or charge to either Purchasing Entity or Purchasing Entity’s transferee.

The rights of a Participating Entity and its authorized Purchasing Entities in the products and services being provided under this Master Agreement shall be for purposes of each Participating Entities’ and Purchasing Entities’ internal business only (which includes use by third parties doing business with each entity, to the extent contemplated in the RFP) during the term of this Master Agreement. All other intellectual property rights in the Products and services remain in and/or are assigned to Contractor. Where software is provided with a product or Service, the Participating Entity and its authorized Purchasing Entities are granted a non-exclusive, fully paid, royalty free, perpetual license to use the software, including any related Product, solely to enable use of the products and services to achieve the purposes of the Master Agreement.

19. Intentionally Omitted

General Provisions

20. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers with the appropriate jurisdictional authority to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of A.M. Best's Insurance Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below:

> (1) Commercial General Liability covering premises operations, any person or organization working on behalf of the Contractor, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$2 million general aggregate;
>
> (2) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

c. Contractor shall pay premiums on all insurance policies. Contractor shall provide notice to a Participating Entity who is a state within five (5) business days after Contractor is first aware of expiration, cancellation or nonrenewal of such policy or is first aware that cancellation is threatened or expiration, nonrenewal or expiration otherwise may occur.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) includes the Participating States identified in the Request for Proposal as additional insureds, (2) provides that written notice of cancellation shall be delivered in accordance with the policy provisions, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, other state Participating Entities' rights and Contractor's obligations are the same as those specified in the first sentence of this subsection except the endorsement is provided to the applicable state.

e. Contractor shall furnish to the Lead State copies of certificates of all required insurance in a form sufficient to show required coverage within thirty (30) calendar days of the execution of this Master Agreement and prior to performing any work. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date to the applicable state Participating Entity. Failure to provide evidence of coverage may, at the sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum, respectively.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

21. Records Administration and Audit

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and Orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Upon reasonable prior written notice (at least ten (10) business days, Contractor shall permit at Contractor's business offices during normal business hours the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency (collectively the "Auditing Authorities"), to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or Orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of five (5) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, or such longer period as is required by the Purchasing Entity's state statutes, to assure compliance with the terms hereof or to evaluate performance hereunder. Further, due to the highly sensitive and proprietary nature of Contractor's records, any third party auditor acting on behalf of the Auditing Authorities shall be subject to prior approval by Contractor, which shall not be unreasonably withheld, and may be required at Contractor's sole discretion to execute Contractor's standard Non-Disclosure Agreement prior to examining, inspecting, copying or auditing Contractor's records. Such non-disclosure agreement shall not prohibit disclosure to the Lead State or discussion between the third-party auditor and the Lead State for the purposes of performing an audit.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or Orders or the Purchasing Entity or NASPO ValuePoint for underpayment of Contractor's Administrative Fees found as a result of the examination of the Contractor's records so long as (i) a claim for such reimbursement is sent to the Contractor within 90 days of completion of the audit; (ii) Contractor is provided a written explanation as to the reasons payment was considered inconsistent with the terms of the Master Agreement; and (iii) Contractor agrees with the written explanation. The Lead State, Participating Entity, or Purchasing Entity (as applicable) will agree to cooperate with Contractor to resolve any dispute as to the claim(s) for overpayments or underpayment of fees. Either party may invoke the negotiation process outlined in the Dispute Resolution section of Attachment AA Contractor's Additional Terms and Conditions to resolve such dispute.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations. Contractor agrees to keep and maintain full, true, and complete billing records, books, and documents as practicable to disclose to the Lead State or their authorized representatives, upon audits, sufficient information to reasonably determine compliance with this Master Agreement and all state regulations and statutes.

22. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity or Purchasing Entity's end users or clients. Any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity records, (2) personnel records, and (3) personally identifying information, is confidential information of Purchasing Entity ("Confidential Information"). Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of the Lead State or Purchasing Entity.

e. The rights granted Purchasing Entities and Contractor obligations under this section shall also extend to NASPO ValuePoint's Confidential Information, defined to include Participating Addenda, as well as Orders or transaction data relating to Orders under this Master Agreement that identify the entity/customer, Order dates, line item descriptions and volumes, and prices/rates. This provision does not apply to disclosure to the Lead State, a Participating State, or any governmental entity exercising an audit, inspection, or examination pursuant to section 20. With the exception of legal demands relating to law enforcement or national security subpoenas, wiretaps, or court orders and to the extent permitted by law or regulation, Contractor shall notify the Lead State of the identity of any entity seeking access to the Confidential Information described in this subsection.

23. Public Information

This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

24. Assignment/Subcontracts

a. Contractor shall not assign, sell, transfer, subcontract or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State which consent shall not be unreasonably withheld, conditioned, or delayed. Notwithstanding the foregoing, the parties acknowledge and agree that the Contractor may assign this Master Agreement to a parent company, controlled affiliate under common control or an entity that has purchased substantially all of its assets upon written notice to the Lead State.

b. The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to NASPO ValuePoint and other third parties.

25. Changes in Contractor Representation

The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel managing the Master Agreement in writing within 10 business days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal, which shall not be unreasonably withheld, conditioned or delayed. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

26. Independent Contractor

The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

27. Cancellation

a. Cancellation for Convenience. Unless otherwise stated, this Master Agreement may be canceled for convenience by either party upon 60 days written notice prior to the effective date of the cancellation. Further, any Participating Entity or Purchasing Entity may cancel its participation for convenience upon 30 days written notice to Contractor, unless otherwise limited or stated in the Participating Addendum. Cancellation may be in whole or in part. Any cancellation under this provision shall not affect the rights and obligations attending orders outstanding at the time of cancellation, including any right of a Purchasing Entity to indemnification by the Contractor, rights of payment for Products delivered and accepted as provided for in this Section 27, rights attending any warranty or default in performance in association with any Order, and requirements for records administration and audit.

b. Cancellation for Non-appropriation. Participating Entity or Purchasing Entity under a Participating Addendum or an Order may cancel, without incurring any form of payment liability in excess of previously appropriated amounts, only when Participating Entity or Purchasing Entity is unable to secure or allocate sufficient funds in its operating budget to fulfill its financial obligations under a Participating Addendum or an Order for the following fiscal year ("Cancellation for Non-appropriation"). Following Cancellation for Non-appropriation, Participating Entity or Purchasing Entity will not be obligated for payments for any fiscal period after the effective date of cancellation. Participating Entity or Purchasing Entity will give Contractor written notice of any cancellation for non-appropriation at least 30 days before the effective date of the cancellation. At Contractor's request and to the extent possible, Participating Entity or Purchasing Entity will provide supplemental documentation regarding the non-appropriation of funds. Participating Entity or Purchasing Entity must take all necessary action to budget and secure any funds required to fulfill its contractual obligations for each fiscal year during the Term.

c. Contractor Right to Suspend or Cancel a Participating Entity or Purchasing Entity for Cause**.** Contractor may suspend or cancel Products or Services, a Participating Addendum or an Order immediately if Participating Entity or Purchasing Entity: (i) fails to cure a payment default within 15 days of receiving Contractor's written notice of nonpayment; (ii) fails to cure any other material breach within 30 days after receiving Contractor's written notice; (iii) provides false or deceptive information or engages in fraudulent or harassing activities when ordering, using or paying for Products or Services; (iv) fails to comply with applicable law or regulation and it's noncompliance materially interferes with Contractor's performance under the Participating Addendum or an Order or exposes Contractor to legal liability; or (v) fails to comply with the resell restrictions contained in the Master Agreement. If Participating Entity or Purchasing Entity under a Participating Addendum or an Order disputes the basis for Contractor's suspension or cancellation, Participating Entity or Purchasing Entity under a Participating Addendum or an Order must invoke the negotiation process outlined in the Dispute Resolution section of Attachment AA.

d. Effect of Cancellation of a Participating Entity or Purchasing Entity**.** If, before the end of a Pricing Term, defined in Attachment AA, Contractor cancels a Product, Service, or an Order under the Suspension or Cancellation for Cause section of this Master Agreement, or if Participating Entity or Purchasing Entity under an Order cancels a Product, Service or an Order under this Section 27 of this Master Agreement, Participating Entity or Purchasing Entity will pay Contractor (A) for any Products and Services provided up to and including the date of cancellation, whether or not billed by the cancellation date, as well as any applicable early termination fees, any applicable shortfall liabilities and other applicable charges and fees, as set forth in this Master Agreement, and (B) a pro rata portion of any credits issued (excluding service outage credits) or charges waived, based upon the number of months remaining in any applicable order term or minimum service term at the time of cancellation.

e. Effects of Cancellation of Individual Responsible (IRU) Accounts. IRU accounts who sign Contractor's consumer subscriber agreement are subject to the order term requirements and other obligations in the separate subscriber agreement between Contractor and the Employee.

28. Force Majeure

Neither party to this Master Agreement shall be held responsible for delay or non-performance caused by acts, events or causes which are beyond that party's reasonable control (a "Force Majeure Event"). Force Majeure Events include, but are not limited to, natural disasters such as fire, unusually severe weather or other acts of God; war, riots and terrorist activities. The Lead State may terminate this Master Agreement for convenience pursuant to Section 27 after determining such delay or non-performance will reasonably prevent successful performance of the Master Agreement.

29. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or
(2) A material breach of any term or condition of this Master Agreement; or
(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or
(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or
(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, the Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default, Unless the default poses a risk to human health or safety, in which case a commercially reasonable shorter cure may be set by the Lead State (which shall not be less than five (5) business days). Time allowed for cure shall not diminish or eliminate Contractor's liability for damages to the extent not otherwise limited under this Master Agreement.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and the Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and
(2) Terminate this Master Agreement and any related Contracts or portions thereof; and
(3) Suspend Contractor from being able to respond to future bid solicitations; and
(4) Suspend Contractor's performance; and
(5) Withhold disputed payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and shall have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Unless otherwise specified in a Purchase Order, a Purchasing Entity shall provide written notice of default as described in this section and have all of the rights and remedies under this paragraph and any applicable Participating Addendum with respect to an Order placed by the Purchasing Entity. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable State law.

30. Waiver of Breach

Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

31. Debarment

The Contractor certifies that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

32. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers and employees, from and against third-party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property arising from the negligent or willful act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement. Contractor will not be liable for damages to the extent that they are the result of negligence or willful misconduct by NASPO, the Lead State, the Participating Entities, Purchasing Entities, and/or their respective employees, officers, and authorized agents.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint), the Lead State, Participating Entities, Purchasing Entities, along with their officers and employees ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or Services, or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor.

Control of Defense:
If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it; however, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible (and such consent shall not be unreasonably withheld).

If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim.

The Party controlling such defense shall keep the other party advised of the status of such action, suit, proceeding or claim and the defense thereof and shall consider recommendations made by the other party with respect thereto.

Cooperation among the Parties:
The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for Contractor's defense of the action or proceeding.

The Indemnified Party may, at its option and expense, be represented by counsel of its choice in any action or proceeding with respect to such Claim; and Contractor and its legal counsel shall cooperate with the Indemnified Party and its legal counsel in providing such information as the Indemnified Party may reasonably request, in support of its defense.

Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

(3) Contractor's obligations under this section will not apply to the extent that the infringement or violation is caused by (i) Contractor's creation of software or hardware using functional or other specifications that were provided by or requested by the Indemnified Party; or (ii) the Indemnified Party's continued use of infringing

Products or services after Contractor provides reasonable notice to the Indemnified Party of the infringement and Contractor requested in writing that the Indemnified Party cease use of the infringing Products or services. For any third party claim that Contractor receives, or to minimize the potential for a claim, Contractor may, at its option and expense, either: (A) procure the right for the Indemnified Party to continue using the Products or services; (B) replace or modify the Products or services with comparable Products or services; or (C) if neither previous option is reasonably practicable, terminate the Products or services. The provisions of this Section state the entire liability and obligations of Contractor and any of its affiliates or licensors, and the exclusive remedy of State, with respect to any actual or alleged infringement in whole or in part, of any patent, copyright, trade secret, trademark or other intellectual property right by the Products or services.

33. No Waiver of Sovereign Immunity

In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of the Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating Entities who are states only to the extent Congress has appropriately abrogated the state's sovereign immunity and is not consent by the state to be sued in federal court. This section is also not a waiver by the state of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

34. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State. The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; a Participating State if a named party; the state where the Participating Entity or Purchasing Entity is located if either is a named party.

35. Assignment of Antitrust Rights

Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided in that state for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at the Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action. Notwithstanding the foregoing, the parties acknowledge and agree that Contractor assigns such causes of action to a Participating Entity to the extent a Participating Entity can demonstrate that it has either (1) paid monies not otherwise due or (2) received less compensation than it would otherwise have been entitled to receive as a result of violations of federal or state antitrust laws.

36. Contract Provisions for Orders Utilizing Federal Funds

Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation of applicable provisions of Appendix II to 2 Code of Federal Regulations (CFR) Part 200 in Orders placed under this Master Agreement.

37. Leasing or Alternative Financing Methods

The procurement and other applicable laws of some Purchasing Entities may permit the use of leasing or alternative financing methods for the acquisition of Products under this Master Agreement. Where the terms and conditions are not otherwise prescribed in an applicable Participating Addendum, the terms and conditions for leasing or alternative financing methods are subject to negotiation between the Contractor and Purchasing Entity.

38. Limitations of Liability

The parties are commercial entities and acknowledge that each has had the opportunity to seek advice from counsel pertaining to this Agreement.

a. **Damage Limitations.** Each party's maximum liability for damages to the other party caused by its failure(s) to perform its obligations under this Agreement is limited to: (A) proven direct damages for claims arising out of personal injury or death, damage to real or personal property, or the release of non-public Purchasing Entity data, subject to applicable liability caps under state or federal regulation/law, caused by the party's negligent or willful misconduct; and (B) proven direct damages for all other claims arising out of this Agreement, not to exceed in the aggregate, in any 12 month period, an amount equal to Customer's total net payments for the affected Services purchased in the six months prior to the event giving rise to the claim. Customer's payment obligations, liability for early termination charges, and the parties' indemnification obligations under this Agreement are excluded from this provision.

b. Damage Waivers.

(1) NEITHER PARTY WILL BE LIABLE FOR ANY LOST PROFITS (INCLUDING LOST REVENUE AND LOSS OF BUSINESS OPPORTUNITY, AND REGARDLESS OF THE THEORY FOR RECOVERY), OR ANY CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES FOR ANY CAUSE OF ACTION, WHETHER IN CONTRACT OR TORT, WHETHER FORESEEABLE OR NOT.

(2) Contractor is not liable (i) for unauthorized third party access to, or alteration, theft or destruction of, Customer's data, programs or other information through accident, wrongful means or any other cause while such information is stored on or transmitted across Sprint network transmission facilities or Customer premise equipment; (ii) for the content of any information transmitted, accessed or received by Customer through Sprint's provision of the Products and Services, excluding content originating from Sprint; or (iii) if a commercially reasonable change in Products or Services causes equipment or software not provided by Sprint to become obsolete, require alteration, or perform at lower levels.

ATTACHMENT AA – CONRACTOR'S ADDITIONAL TERMS AND CONDITIONS

The following items are incorporated into this Attachment AA:

1. Contractor's Additional Terms and Conditions
2. Contractor's Product/Service Annexes

Nothing contained in this Attachment AA will be deemed to modify, diminish, or otherwise derogate the terms and conditions set forth in the Master Agreement, except to the extent required by law. If a conflict exists among the provisions within the documents that form this Attachment, the following order of precedence will apply: 1) Contractor's Additional Terms and Conditions; and 2) Contractor's Product/Service Annexes.

CONTRACTOR'S ADDITIONAL TERMS & CONDITIONS

1. GENERAL.

1.1 For the purposes of this Contractor's Additional Terms and Conditions and any Contractor's Product and Service Annexes incorporated into the Master Agreement, as attached hereto as Attachment AA to the Master Agreement, "Sprint" means **SPRINT SOLUTIONS, INC.**, as contracting agent on behalf of the applicable Sprint affiliated entities providing the Products and Services, and "Customer" means the applicable Purchasing Entity under an Order.

2. CHARGES

2.1. Pricing. If Customer purchases a Product or Service that is not priced in this Master Agreement, Customer's pricing will be based on Sprint's then-current list price at the time of purchase. Unless expressly stated otherwise, the pricing may not be available if an indirect sales agent is involved in the transaction.

2.2. Rate Adjustments. Sprint may impose on Customer additional regulatory fees; administrative charges; and charges, fees or surcharges for the costs Sprint incurs in complying with governmental programs. These fees, charges or surcharges may include state and federal Carrier Universal Service Charges ("CUSC"), Compensation to Payphone Providers, Telephone Relay Service, or Gross Receipts surcharges, and the amounts may vary. If the Federal Communications Commission ("FCC") requires that Sprint contribute to the Universal Service Fund ("USF") based on Services that Sprint in good faith has treated as exempt, Sprint will bill Customer the CUSC for such Services beginning on the date the FCC establishes such Services became subject to USF contributions.

2.3. Taxes. Sprint's rates and charges for Products and Services do not include taxes, nor do the rates and charges contemplate that taxes will be deducted or withheld by Customer from the payments Customer makes to Sprint. Customer will pay all taxes, including, but not limited to, sales, use, gross receipts, excise, VAT, property, transaction, or other local, state or national taxes or charges imposed on, or based upon, the provision, sale or use of Products or Services. Customer will not deduct any withholding taxes (or taxes deducted at the source) from any invoiced amounts. Customer will pay Sprint as if no withholding taxes were applied, and will additionally pay any withholding taxes to the relevant authorities in accordance with applicable law. Customer will not be responsible for payment of Sprint's direct income taxes, employment taxes, and any other tax to the extent that Customer demonstrates a legitimate exemption under applicable law. Sprint will honor any valid tax exemptions provided to Sprint by Customer. Additional information on the taxes, fees, charges, and surcharges collected by Sprint is posted on the Rates and Conditions Website: http://www.sprint.com/business/support/ratesWelcome.html.

2.4 Pricing Term. The pricing and discounts set forth in the Master Agreement will expire based on the term designated by the Purchasing Entity in an individual Order ("Pricing Term"). Following the expiration of the Pricing Term, Sprint will continue to provide wireless Products and Services to Customer under the pricing and discounts set forth in the Master Agreement, or, with 30 days' advance notice to Customer, at standard list pricing, until either party provides 30 days' advance written notice to terminate wireless Services. If Customer Lines (as defined in this Attachment) are subject to a Minimum Service Term (as defined in this Attachment) as of the expiration of the Pricing Term, those Customer Lines will continue to receive the pricing and discounts set forth in the Order until the earlier of the expiration of the applicable Minimum Service Term or the termination of Wireless Services.

2.5. **Wireless Devices.** To access Sprint wireless Services, Customer may utilize wireless devices purchased from Sprint, wireless devices leased from Sprint, wireless devices obtained from Sprint as part of a Product or Service bundle, or wireless devices provided by Customer.

A. **Purchased Devices.** If Customer purchases wireless devices from Sprint, Customer may pay (1) full Suggested Retail Price ("SRP"), (2) a discounted device price in exchange for Customer keeping the device active for a minimum period of time ("Subsidized Devices"), or (3) SRP for the cost of the device through monthly installments ("Monthly Installments"). To pay for wireless devices via Monthly Installments, Customer must sign a separate Installment Agreement with Sprint.

B. **Leased Devices.** If Customer leases wireless devices from Sprint, Customer must enter into a separate Business Lease Agreement with Sprint and title to the devices will remain with Sprint unless Customer exercises the purchase option set forth in the Business Lease Agreement.

C. **Unsubsidized Devices.** All wireless devices that are not Subsidized Devices are considered "Unsubsidized" devices.

D. **SIM Cards.** For International M2M Services, Customer must purchase SIM Cards from a Sprint-authorized third party.

2.6 **Wireless Minimum Service Term Requirement.** Wireless Services may require a device or Business Plan to remain active for a minimum period of time ("Minimum Service Term"). The Minimum Service Term begins on the wireless device purchase date and ends on the expiration of the device Minimum Service Term or the Business Plan Minimum Service Term, whichever is later. The applicable Minimum Service Term(s), if any, are available at Customer's My Sprint Business account or by contacting Customer's Sprint Account Representative.

2.7 **Wireless Device Discount; Upgrade Terms; Exclusions**.

A. **Wireless Device Discount.** New Customer Lines may be eligible for a discounted device price with a device Minimum Service Term of 24 months. Sprint may offer different discounted device prices for devices with different device Minimum Service Terms. The devices offered with this discounted device price may change at any time in Sprint's sole discretion. This discounted device offer may not be available in all sales channels.

B. **Upgrade Terms.** Customer will receive the discounted device price described in subsection A above when upgrading or replacing a Subsidized Device that has been in service for at least 24 continuous months. The upgraded or replacement device may be subject to a new device Minimum Service Term. Sprint may offer a different device price for Subsidized Devices that have not been in service for 24 continuous months, or for Unsubsidized devices. More information is available by contacting Customer's Sprint Account Representative.

C. **Exclusions.** The discounted device price does not apply to certain devices or Unsubsidized devices ("Excluded Devices"). The discounted device price and device Minimum Service Term, if any, for Excluded Devices are available by contacting Customer's Sprint Account Representative and may change at any time in Sprint's sole discretion.

2.8 **Government Service Pricing Discount Program**.

A. **Government Service Pricing Discount**. The Government Service Pricing Discount is a percentage discount off the eligible monthly recurring charges ("MRCs") charged for Customer Lines. Employee Lines are eligible for the Employee Discount included in the Employee Discount Program Section of this Attachment after contacting a Sprint representative and meeting the eligibility requirements in the Eligible Employees Section of this Attachment.

B. **Effective Date of Government Service Pricing Discount.** For Customer Lines activated during the Pricing Term, the Government Service Pricing Discount applies no later than 60 days after the date of activation. For Customer Lines activated under a prior agreement between Sprint and Customer, Sprint will apply the Government Service Pricing Discount no later than 60 days after the effective date of the Pricing Term.

C. **Application of Government Service Pricing Discount.** Unless otherwise noted in the terms of the applicable Business Plan, the Government Service Pricing Discount applies to eligible monthly recurring charges ("MRC") before taxes and surcharges and after application of credits, other discounts and rebates. Overage, usage-based, third party applications and services, certain Business Plans and Business Plan add-ons, and other charges are not eligible for the Government Service Pricing Discounts. The Government Service Pricing Discount may apply to the MRC of certain promotional rate plans, which Sprint may offer on a limited time basis, at Sprint's discretion. Only Customer Lines that are included in Customer's Sprint account hierarchy are eligible for the Government Service Pricing Discount. Customer's contractors, suppliers, and any non-government, non-authorized agencies working with Customer are not eligible for the Government Service Pricing Discount.

2.9 **Accessory Discount.** Customer will receive a 25% discount off of the national retail price for select accessories purchased for Customer Responsible (CRU) or Individual Responsible (IRU) accounts.

2.10 **Shipping Fees.** Sprint will waive standard shipping fees for Customer Lines. Additional charges may apply for overnight or expedited shipping. Shipping fees for IRU accounts shall be governed by the terms of Sprint's consumer subscriber agreement.

2.11 **Activation Fees.** In accordance with Attachment B, Scope of Work, Section 2.1.6 Service Requirements, Sprint will waive the nonrefundable activation fee for each CRU and IRU billing account that Sprint creates during the term.

2.12 **Reactivation Fees.** In accordance with Attachment B, Scope of Work, Section 2.1.6 Service Requirements, Sprint will waive the reactivation charge for each CRU and IRU before Sprint reactivates service to the affected Device.

2.13 **Early Termination Fees.** In accordance with Attachment B, Scope of Work, Section 2.1.6 Services Requirements, Sprint will waive the early termination fee for Subsidized Devices for any Customer Line terminated prior to 24 months of continuous service. If Customer purchases wireless devices via Monthly Installment or leases wireless devices from Sprint, early termination fees shall apply as set forth in the separate Installment Agreement or the Business Lease Agreement, as applicable. Early termination fees for IRU accounts shall be governed by the terms of Sprint's consumer subscriber agreement.

3. ORDERS, BILLING AND PAYMENT

3.1. **Customer Orders.** Customer is responsible for all Orders issued under this Master Agreement. Sprint may accept an Order by (A) signing and returning a copy of the Order to Customer; (B) delivering any of the Products or Services ordered; (C) informing Customer of the commencement of performance; or (D) returning an acknowledgment of the Order to Customer. The terms and conditions in any Customer-generated Order template will have no force or effect other than to denote quantity, the Products or Services purchased or leased, delivery destinations, requested delivery dates and any other information required by this Agreement. Customer may cancel an Order at any time before Sprint ships the Order or begins performance, but Customer will pay any actual costs related to the provisioning of Products and Services, including but not limited to shipping, incurred by Sprint due to Customer's cancellation. Sprint may reject or cancel an Order for any reason. Sprint will promptly notify Customer of rejected or canceled Orders.

3.2. **Billing.** In general, for recurring Services, Sprint bills fixed Service charges in advance and usage-based charges in arrears. Depending on the Product or Service ordered, Sprint may begin billing Customer on the date the Products or Services are made available to Customer, or on the delivery date specified in the Order. If Sprint cannot make available a Product or Service due to a Customer-caused delay, Sprint may bill Customer as of the delivery date specified in the Order or, if no date is specified, any time 30 days or more after Sprint receives the Order. **Unless**

otherwise agreed by the parties in writing, Sprint will bill Customer electronically and will notify Customer via email when the bill is available for viewing.

3.3. **Payment Terms.** For the Products and Services acquired under this Agreement, Sprint will bill Customer, and Customer will pay Sprint, in United States dollars (USD). Payment terms are net 30 days from the date of invoice receipt (the "Due Date"). Except as provided in the Disputed Charges section below, if Customer fails to pay all amounts due by the Due Date, then Sprint reserves the right to charge a late fee (up to the maximum allowed by law). Customer may not offset credits owed to Customer on one account against payments due on the same or another account. Sprint's acceptance of late or partial payments is not a waiver of its right to collect the full amount due. Customer's payment obligations include late charges and third party collection costs incurred by Sprint to collect past due amounts, including reasonable attorneys' fees. Customer agrees to remit payments using cash, check, or electronic fund transfer. Customer must contact its assigned Sprint representative to use an alternative form of payment.

3.4. **Disputed Charges.** If Customer disputes a charge in good faith, Customer may withhold payment of that charge if Customer (A) pays all undisputed charges on or prior to the Due Date; and (B) within 30 days of the Due Date, provides Sprint with a written explanation of Customer's reasons for disputing the charge. Customer must cooperate with Sprint to resolve promptly any disputed charge. If Sprint determines, in good faith, that the disputed charge is valid, Sprint will notify Customer and, within five business days of receiving notice, Customer must pay the charge or invoke the negotiation process outlined in the Dispute Resolution section of this Attachment. If Sprint determines, in good faith, that the disputed charge is invalid, Sprint will credit Customer for the invalid charge.

3.5. **Payment History.** Sprint's provision of Products and Services is subject to Sprint's credit approval of Customer. If Customer's financial circumstance or payment history is or becomes reasonably unacceptable to Sprint, then Sprint may require adequate assurance of future payment as a condition of providing Products and Services to Customer. Sprint may provide Customer's payment history or other billing/charge information to any credit reporting agency or industry clearinghouse.

4. EQUIPMENT AND SOFTWARE

4.1. **Non-Sprint Equipment or Software.** Customer is responsible for curing any impairment to Product or Service quality that is caused by equipment or software not provided by Sprint. Customer will continue to pay Sprint for Products and Services during such impairment.

4.2. **Software License.** Customer is granted a non-exclusive and non-transferable license or sublicense to use software provided with a Product or Service, in accordance with the applicable software licensing terms. No rights are granted to source code. Customer cannot use any software on behalf of third parties or for time share or service bureau activities and cannot reverse engineer, decompile, modify, or enhance any software. Sprint may block or terminate Customer's use of any software if Customer fails to comply with applicable licensing terms.

5. USE OF PRODUCTS AND SERVICES

5.1 **Acceptable Use Policy.** If Customer uses Products or Services, Customer must conform to the acceptable use policy posted at http://www.sprint.com/legal/agreement.html, as reasonably amended from time to time by Sprint. Customer will prevent third parties from gaining unauthorized access to the Products and Services via Customer's facilities.

6. CPNI; TRADEMARKS; AND FOIA

6.1 **Customer Proprietary Network Information; Privacy.** As Sprint provides Products and Services to Customer, Sprint develops information about the quantity, technical configuration, type and destination of Products and Services Customer uses, and other information found on Customer's bill ("Customer Proprietary Network Information" or "CPNI"). Under federal law, Customer has a right, and Sprint has a duty, to protect the confidentiality of CPNI. Sprint's privacy policy, as amended from time to time, includes information about Sprint's CPNI and other data practices and can be found at www.sprint.com/legal/privacy.html.

6.2 **Use of Name, Service Marks, Trademarks.** Except as provided in the Section below, neither party will use the name, service marks, trademarks, or carrier identification code of the other party or any of its Affiliates for any purpose without the other party's prior written consent.

6.3 **FOIA.** Sprint acknowledges that the Agreement and the Confidential Information may be subject to disclosure in whole or in part under applicable Freedom of Information, Open Records, or Sunshine laws and regulations (collectively "FOIA"). To the extent permitted by applicable law, Customer will provide Sprint with prompt notice of any FOIA requests or intended disclosures for confidential or proprietary information, including citations to or copies of applicable FOIA for review, and an appropriate opportunity to seek protection of Sprint Confidential Information. A Participating Entity or Purchasing Entity shall have no obligation to provide Sprint with notice or any request or disclosure for information that is already in the public realm or otherwise publicly available.

7. INDEMNIFICATION (AUTHORIZED NON-PROFIT ENTITIES)

This Indemnification Section of Attachment AA applies only to Purchasing Entities who are authorized 501(c)3 non-profit entities.

7.1. **Mutual Indemnification for Personal Injury, Death or Damage to Personal Property.** Each party will indemnify and defend the other party, its directors, officers, employees, agents and their successors against all claims for damages, losses, liabilities or expenses, including reasonable attorneys' fees, brought against the indemnified party by a third party (collectively, "Claims"), arising directly from the indemnifying party's performance of this Agreement and relating to personal injury, death, or damage to tangible personal property to the extent such Claims are alleged to have resulted from the negligence or willful misconduct of the indemnifying party or its subcontractors, directors, officers, employees or authorized agents.

7.2. **Customer Indemnification.** Customer will indemnify and defend Sprint, Sprint's directors, officers, employees, agents and their successors, against all Claims arising out of (A) Customer's breach of the licensing requirements in the Software License section; (B) Customer's failure to comply with any provision of the Use of Products and Services section; (C) Customer's infringement of patents arising from the use of equipment, hardware or software not provided by Sprint; or (D) Sprint's failure to pay any tax based on Customer's claim of a legitimate exemption under applicable law.

7.3. **Sprint Indemnification.** Sprint will indemnify and defend Customer, Customer's directors, officers, employees, agents and their successors against Claims enforceable in the United States alleging that Services as provided infringe any third party United States patent or copyright or contain misappropriated third party trade secrets. Sprint's obligations under this section will not apply to the extent that the infringement or violation is caused by (A) functional or other specifications that were provided or requested by Customer, or (B) Customer's continued use of infringing Services after Sprint provides reasonable notice to Customer of the infringement. For any Claim that Sprint receives, or to minimize the potential for a Claim, Sprint may, at its option, either: (i) procure, at Sprint's expense, the right for Customer to continue using the Services; (ii) modify the Services or replace the Services with comparable Services, each at Sprint's expense; or (iii) terminate the Services.

7.4. **Rights of Indemnified Party.** The party seeking indemnification must (A) give the indemnifying party timely written notice of the Claim, (B) give the indemnifying party full and complete information, assistance and authority for the Claim's defense and settlement, and (C) not, by any act, admission or acknowledgement, materially prejudice the indemnifying party's ability to satisfactorily defend or settle the Claim. The indemnified party may participate in the settlement or defense of the Claim, with its own counsel and at its own expense; provided that the indemnifying party will retain the right to settle or defend the Claim, in its sole discretion, at its own expense and with its own counsel. Notwithstanding the foregoing, the indemnifying party will not make, without the prior approval of the indemnified party, which approval will not be unreasonably withheld, any admission of facts on behalf of the indemnified party that exposes the indemnified party to the imposition of punitive damages or exposure to other claims that are not covered by this indemnification.

8. TECHNOLOGY EVOLUTION

8.1. In the normal course of technology evolution and enhancement, Sprint continually updates and upgrades its networks, Products and Services. In some instances, these efforts will result in the need to ultimately replace or discontinue certain offerings or technologies. In such event, Sprint will undertake such efforts in a customer-focused and commercially reasonable manner. Accordingly and notwithstanding anything in this Master Agreement to the contrary, Sprint reserves the right, in its sole discretion, after providing the notice set forth in subsection (2) below, to: (a) migrate Customer to a replacement technology; or (b) discontinue any Product, Service, network standard, or technology without either party being in breach of this Master Agreement or incurring early termination liability relating to the discontinuance of the affected Product, Service, network standard, or technology.

8.2. If Sprint takes any action set forth in subsection (1) above, Sprint will provide no less than 60 days' advance notice reasonably designed to inform Customer (if affected) of such pending action. The form of Sprint's notice may include providing written notice to any address (a) listed in the Participating Addendum for Customer, (b) Sprint uses for billing, or (c) set forth in an Order. Customer agrees that such notice is reasonable and sufficient notice of Sprint's pending action.

9. **NOTICES.** Notices required under this Agreement must be submitted in writing to any address listed in this Agreement for the other party, or for notices to Customer, to the address Sprint uses for shipping or billing or as set forth in an Order. In the case of a dispute, notices also must be sent to:

Sprint
Attn: Legal Dept. – Public Sector
12502 Sunrise Valley Drive
MS: VARESA0208
Reston, VA 20196

Attn: VP Legal Dept. – Sales & Distribution
Mailstop: KSOPHT0101-Z2525
6391 Sprint Parkway
Overland Park, KS 66251-2525

10. DISPUTE RESOLUTION

10.1. **Negotiations.** In the event of a dispute arising from or relating to this Master Agreement, the disputing party will notify the other party in writing. The parties will negotiate with each other in good faith and will use their best efforts to resolve the dispute within 15 days of the notice date. If the dispute is not resolved within this 15 day period, each party will escalate the dispute to higher management (VP or equivalent). If the dispute is not resolved within 30 days after the escalation, either party is free to seek relief as contemplated in this Master Agreement.

11. EMPLOYEE DISCOUNT PROGRAM

11.1. Employee Discount Program.

A. Eligible Employees. Employees who: i) sign Sprint's consumer subscriber agreement; ii) purchase Products and Services on an IRU account: and iii) provide to Sprint satisfactory evidence of employment with Customer, will be eligible to receive a financial benefit ("Employee Discount"). The Employee Discount may be in the form of a fixed dollar consumer rate plan discount, a gift card or other similar offer, or a percentage discount applied to eligible Sprint consumer rate plans before taxes and surcharges. Overage, usage-based, third party applications and services, and other charges are not eligible for the Employee Discount. Customer will use commercially reasonable efforts to comply with Sprint's employment verification requests and methods. Upon (1) termination of this Master Agreement for any reason, (2) an Employee's termination of employment with Customer, or (3) Sprint's determination that an Employee is not in compliance with the consumer subscriber agreement, Sprint may cease providing the Employee Discount. In addition, Sprint reserves the right to discontinue offering the Employee Discount for new Sprint accounts activated following expiration of the Pricing Term. Except for the conditions set forth above, Employee Lines are governed exclusively by the terms and conditions in the consumer subscriber agreement, including those terms and conditions relating to the applicability of the Employee Discount to rate plans, promotions or other special offers. Current offer information is available by contacting Customer's Sprint Account Representative.

B. Communications. Sprint and Customer's designated employee benefits group will develop and agree to a communications plan to present discounts and sell to Employees within 60 days of the Effective Date. Communications may be include new hire materials, benefits enrollment materials, email, payroll stuffers, newsletters, internet and intranet links, chair drops, or other mutually agreed to methods.

12. ELECTRONIC BILLING PRODUCTS

12.1. The following electronic billing products provide Customer Line call detail record information:

ELECTRONIC BILLING PRODUCTS	Invoice Data	Summary Data	Minimum Customer Lines
Sprint Business Invoice Analytics	3 months	12 months	25
Data Direct	1 month	Not available	100
Electronic Data Interchange (EDI)	1 month	Not available	100

12.2. There are no charges associated with the electronic billing products listed above. Customer may choose any combination of electronic billing products. For Data Direct and Electronic Data Interchange, data is provided for current billing cycles. Archived data is available for as long as the account numbers are enrolled in the electronic billing product. Sprint reserves the right, upon 60 days' prior notice, to decommission a billing product, or to migrate Customer to an updated or successor version of the selected electronic billing product if available or to an entirely new electronic billing product. Electronic Billing Products are not available with International M2M Services or with M2M Devices managed through Command Center or the Orange M2M Portal.

13. ADDITIONAL BUSINESS PLANS AND SPECIAL OFFERS.

14.1 Additional Business Plans. If Customer is eligible for and selects a Business Plan that is not specified in this Master Agreement, the Government Service Pricing Discount may apply to the Business Plan unless otherwise stated in the Business Plan, and the terms and conditions of the Business Plan will apply in addition to, and control over, any conflicting terms or conditions in the Master Agreement.

14.2 **Promotions.** Sprint promotional discounts may not be available with certain Business Plans, as indicated in the promotional offer. If Customer purchases a promotional wireless Product or Service, the promotional terms will control over any conflicting terms in the Master Agreement for that wireless Product or Service until the promotion expires or Customer selects a different Business Plan for the Customer Line enrolled in the promotion.

14.3 **Trial Offers.** If Customer receives a wireless Service or Service option for a limited trial period at a reduced cost, upon expiration of the trial period, Customer will continue to receive the wireless Service or Service option at full price. If Customer wishes to avoid being billed in full for the promotional wireless Service or Service option, Customer must contact Sprint before the end of the trial period to discontinue the wireless Service or Service option.

14.4 **Business Plans and Features.** Certain wireless Products require specific Business Plans for operation on the Sprint Networks or the Sprint 4G Network. Certain Business Plans, add-ons, features and equipment discounts may not be available on all wireless Products. More information is available by contacting Customer's Sprint Account Representative.

14. ADDITIONAL TERMS

14.1. **Product Annexes/Applicability.** Customer's use of Sprint Products or Services is governed by the applicable Product and Service annexes as posted to the Rates and Conditions Website. All Customers shall comply with the Wireless Services Product Annex. If Customer is utilizing M2M Devices or an electronic billing product, Customer shall comply with the Sprint Machine-to-Machine Services Product Annex and the Electronic Invoice Reporting and Analytics Product Annex. Capitalized terms not otherwise defined in this Attachment shall have the meaning assigned to such terms in the Wireless Services Product Annex, the Sprint Machine-to-Machine Services Product Annex, or the Master Agreement. Notwithstanding the foregoing, the sections of the Machine-to-Machine services Product Annex entitled "INSURANCE" and "INDEMNIFICATION" will not be applicable to Customer.

14.2. **M2M Services.** References in this Attachment to "International M2M Services," "M2M Devices," "Sprint M2M Networks," "M2M Services," an "International M2M Network," the "Orange M2M Portal," and the "Machine-to-Machine Services Product Annex" apply only if Customer is purchasing M2M Services from Sprint.

14.3. **Bundled Service.** Customer may not market or sell M2M Services except in conjunction with an M2M Device and as part of a bundled service offering, which includes other value added services used or sold by Customer.

15. **Education Customers and Programs.** Customers seeking funds through the Universal Service Schools and Libraries Funding Mechanism ("E-Rate Program") or state or local corollaries to the E-Rate Program are subject to the "Schools and Libraries Funding Programs Annex", incorporated by reference.

16. DEFINITIONS

16.1. "Affiliate" is a legal entity that directly or indirectly controls, is controlled by, or is under common control with the party. An entity is considered to control another entity if it owns, directly or indirectly, more than 50% of the total voting securities or other similar voting rights.

16.2. "Customer Line" is the same as "Corporate Liable Active Unit", as defined in the Wireless Services Product Annex, attached hereto.

16.3. "Effective Date" is the date the last party signs the Participating Addendum or Order.

16.4. "Rates and Conditions Website" refers to the website located at http://www.sprint.com/business/support/ratesWelcome.html.

16.5. "Service(s)" means all telecommunications, cloud, software, or other services sold or provided to Customer under this Agreement, excluding Products.

17. MISCELLANEOUS. Subject to the Order of Precedence set forth in the Master Agreement, if a conflict exists among provisions within this Master Agreement, specific terms will control over general provisions, and negotiated, added or attached terms, conditions or pricing will control over standardized, posted or non-negotiated terms, conditions and pricing, to the extent permitted by law. References to Uniform Resource Locators (URLs) in this Master Agreement include any successor URLs designated by Sprint. The terms and conditions of this Master Agreement regarding confidentiality, indemnification, limitations of liability, warranties, payment, dispute resolution and all others that by their sense and context are intended to survive the expiration of this Master Agreement will survive.

ATTACHMENT AA – CONRACTOR’S ADDITIONAL TERMS AND CONDITIONS

CONTRACTOR’S PRODUCT/SERVICE ANNEXES

Purchasing Entity’s use of Sprint Products or Services are also governed by the applicable Product and Service annexes posted on Sprint’s Rates and Conditions website at https://business.sprint.com/terms-and-conditions/. The Product and Services Annexes incorporated into this Agreement are as follows:

Wireless

- Wireless Services Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/wireless_services_product_annex.pdf
- Sprint Machine-to-Machine Services Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/Sprint_M2M_Svs_Prod_Annex.pdf
- Sprint Data Link Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/Data_Link_Product_Annex.pdf
- Emergency Response Team Go-Kit Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/05/ERT-Go-Kit_Product-Annex_-05-04-18.pdf
- Sprint Mobility Management Services Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/mobilityManagementProductAnnex.pdf
- Sprint MultiLine Services Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/04/MultiLine_-_Product_Annex-revised-4.10.2018.pdf

Government and Education

- Schools and Libraries Funding Program Addendum: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/SchoolsandLibrariesFundingProgramAddendum.pdf

Managed, Professional and Other Value-Added Services

- Electronic Invoice Reporting and Analytics Product Annex: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/Electronic_Invoice_Reporting_and_Analytics_Product_Annex.pdf

Sprint Productivity Marketplace Terms of Service

- Software as a Service (SaaS) Terms of Service: https://business.sprint.com/wp-content/uploads/sites/2/2018/03/sprint_software_as_a_service_terms_of_service.pdf

MA262-1

Wireless Data, Voice, and Accessories

Attachment B

Scope of Work

Section 1: General

1.1 Background

The purpose of this Master Agreement is to provide Wireless Data, Voice, and Accessories for all Participating States. The Master Agreement may be used by state governments (including departments, agencies, institutions), institutions of higher education, political subdivisions (i.e., colleges, school districts, counties, cities, etc.), the District of Columbia, territories of the United States, and other eligible entities subject to approval of the individual chief procurement official and compliance with local statutory and regulatory provisions. The initial term of the master agreement shall be 5 (Five) years with renewal provisions for an additional 5 (Five) as outlined in Section 3 of the NASPO ValuePoint Master Terms and Conditions (Attachment A).

1.2 Order of precedence

Per the NASPO ValuePoint Master Terms and Conditions, Participating Addenda (called "PA") will have precedence over the Master Agreement within the participating jurisdiction.

1.3 Green Awards

End users of the Master Agreement may have requirements to purchase products and services that adhere best practices of sustainability and environmental consciousness. Contractor should anticipate addressing these needs as they arise in the Participating Addendum process.

1.4 E-Rate

To the extent the services offered are subject to the E-rate discount program, all award Contract Vendors must commit to participation in the Federal Communication Commission's E-rate discount program established under authority of the Federal Telecommunications Commission Act of 1996. Participation in, and implementation of, this program must be provided without the addition of any service or administration fee by the Contract Vendor.

1.5 Net Neutrality

Recent changes by the Federal Communications Commission in their rules related to the issue of Net Neutrality have increased state's interest in promulgating their own law, rule and policies on this topic. This solicitation will have no requirements related to Net Neutrality for the Master Agreements. It is anticipated, that this issue will be pertinent in the Participating Addendum process. Potential participating entities will be made aware of this consideration by the Lead State in a reasonable fashion.

Section 2: Categories of Award

2.0 Overview of Award Categories

The products and services for this contract are awarded in 3 (three) categories. These categories are:

Category 1- Cellular Wireless Services: This category will cover the basic cellular wireless transport services for voice, data and messaging, as well as any new basic transport services that may be introduced for applications like those defined for Internet of Things (IoT) applications. "Cellular wireless transport" is defined to mean carrier provided wireless services that employ a radio access network based on technologies defined by the Third Generation Partnership Program (3GPP). We are requesting pricing for both traditional cellular plans that include a subsidized mobile device as well as bring your own device (BYOD) plans where the user will supply their own mobile device and require only network service from the carrier.

Category 2- Equipment and Accessories: This category includes any equipment or accessories operating over cellular carrier provided network services or intended for use with cellular connected devices.

Category 3- Turnkey Wireless and IoT Solutions that are offered as a product: This category includes any of the wireless or IoT solutions or applications being offered as a complete product by the cellular wireless carriers or any other Contractor(s).

2.1 Category 1- Cellular Wireless Services

This category will cover the basic cellular wireless transport services for voice, data and messaging, as well as any new basic transport services that may be introduced for applications like those defined for Internet of Things (IoT) applications. “Cellular wireless transport” is defined to mean carrier provided wireless services that employ a radio access network based on technologies defined by the Third Generation Partnership Program (3GPP). We are requesting pricing for both traditional cellular plans that include a subsidized mobile device as well as bring your own device (BYOD) plans where the user will supply their own mobile device and require only network service from the carrier.

This Award Category is for National Award only.

2.1.1 Definitions

3rd Generation Partnership Project (3GPP) The international standards body that covers cellular telecommunications network technologies (http://www.3gpp.org).

3G Third generation of wireless mobile telecommunication technology as defined by the 3rd Generation Partnership Project (3GPP).

4G Fourth generation of wireless mobile telecommunication technology as defined by the 3rd Generation Partnership Project (3GPP).

5G Fifth generation of wireless mobile telecommunication technology as defined by the 3rd Generation Partnership Project (3GPP).

Bandwidth Throttling The mechanism a service provider uses to reduce the data network capacity available to a user of its wireless services.

Bandwidth Throttling Threshold In “unlimited” cellular data plans, the data volume at which the carrier begins instituting bandwidth throttling for the balance of the billing period.

Bring Your Own Device (BYOD) Plans where the user will supply their own mobile device and require only network service from the carrier.

Cellular Wireless Carrier: A wireless carrier that owns the majority of its infrastructure and operates a mobile wireless network primarily utilizing standards developed by the 3GPP.

Cellular Voice A wireless voice telephone service offered by the cellular carriers.

Cellular Wireless Carrier-provided wireless services that employs a radio access network based on technologies defined by the 3rd Generation Partnership Program (3GPP).

Coverage Area The geographic area in which a carrier provides service. When located within this area, a subscriber with a compatible device should be able to access usable wireless services on that carrier’s network or its partner networks.

FirstNet FirstNet is a government subsidized wireless network specifically designed for the needs of public safety users; access to FirstNet services will be limited to defined categories of users related to public safety. FirstNet was created under the Middle Class Tax Relief and Job Creation Act of 2012.

Individual Responsible (IR) Plan Discount Individual Responsible Accounts ("IRU") are accounts for products and services between Contractors awarded a contract under this solicitation and individuals who are employees of eligible users of the Master Agreement. IRU accounts are for the personal use of individual employees of eligible end users of the Master Agreement.

Corporate/Government Responsible (CRU) Plan CRU plans are plans that are purchased by end users of the Master Agreement that is awarded from this solicitation.

Land Mobile Radio (LMR) Terrestrial-based, wireless communications systems, generally operating in the frequency range below 1 GHz, and commonly used by emergency responders to support voice and low-speed data communications.

Mission Critical Push-to-Talk (MCPTT) A new standard for public safety PTT systems (starting with 3GPP Rel. 13) that also operates over the cellular carriers' wireless networks and supports, among other capabilities, the ability for wireless stations to discover and communicate directly with other system users without relaying those transmissions through a cellular base station.

LTE (Long-Term Evolution) A 3GPP standard for high-speed cellular wireless communications.

Mobile Messaging The ability to compose and exchange electronic messages that may include text, audio, video and other symbols between two or more users of mobile phones, tablets or other devices.

Public Safety The functions of government, which ensure the protection of citizens, persons in their territory, organizations, and institutions against threats to their well-being.

Push-to-Talk (PTT) A method of wireless voice communications using a momentary button to switch the wireless device from voice reception mode to transmit mode; in a cellular PTT system, all transmissions are relayed over the carrier's radio channels and through a server installed in the carrier's network infrastructure. Transmissions are received by all stations within range of that particular radio channel and are part of that broadcast group.

Quality of Service (QoS) Mechanisms employed in packet switching networks that allows them to prioritize certain classes of traffic over others thereby providing better performance for those preferred classes with regard to transit delay, jitter (variation in transit delay), and packet loss.

Short Message Service (SMS)/Multimedia Messaging Service (MMS) Wireless services offered by the cellular carriers allowing users to exchange short text (SMS) or audio/video files (MMS). These services are differentiated from other messaging services like Apple Messages and WhatsApp by the fact that they are offered by the cellular carriers and are typically charged as a separate item on the service plan along with voice and data.

Subsidized Plan Cellular plans where the carrier will provide a phone, or tablet at a subsidized price.

Wireless The transmitting of signals using radio waves instead of wires.

Wireless Carrier A provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations.

Wireless Data A communication service offered by mobile carriers that allows users to access the internet and other data services via its wireless networks using a smartphone, tablet or other cellular-connected mobile device.

Wireless Plan A bundled subscription offering from a cellular carrier providing some combination of services.

Wireless Priority Service (WPS) A government-directed emergency phone service managed by the Department of Homeland Security's Office of Emergency Communications (OEC). Like FirstNet for data services, WPS provides priority network access to wireless voice service (2G or VoLTE) exclusively to defined categories of qualified subscribers.

2.1.2 Subsequent Network Characteristics and Technology

This solicitation covers the addition of new technology and methods that are substantively similar to existing 3G, 4G, and 5G Network characteristics.

2.1.3 Plans

Contractors will define the rate plans to be available under the Master Agreement that results from this solicitation and must provide all details of every plan offered in Attachment G. At a minimum plan details should include the items listed in Attachment G if applicable.

Subsidized Plans

Subsidized plans are those that include a device to connect to the wireless network as a part of the monthly plan cost.

Bring Your Own Device Plans

Bring your own device plans are those that require the user to provide a device for connection to the cellular network or to pay for a device separately from the monthly service plan.

2.1.4 Legacy Plans

Plans covered by the predecessor Master Agreements administered by the State of Nevada (Contract No. 1907)("Legacy Plans") for purchasing entities who are currently enrolled will be included within the scope of the Master Agreements awarded by this solicitation. All Legacy Plans must be described on Attachment G: Plan Coverage Attachment.

Discontinuance of Plans

Contractor will maintain plans if they are being used. Contractor may discontinue any plan or feature that has not had any active subscribers for at least the previous 90 days. Contractor to provide a minimum of 90 days notice to Lead State if a Plan is to be discontinued to end users.

2.1.5 Service Requirements

Designated Sales Point of Contact

Each Master Agreement awarded by this solicitation shall have a designated point of contact for sales purposes.

Designated Customer Service Point of Contact

Each Master Agreement awarded by this solicitation shall have a designated point of contact for Customer Service escalation purposes.

Designated Contract Manager

Each Master Agreement awarded by this solicitation shall have a designated point of contact who manages the contract and may be contacted by administrators of the Master Agreement or PAs.

2.1.6 Pricing Requirements

Subsidized Device Plans

Plans covered by the predecessor Master Agreements administered by the State of Nevada (Contract No. 1907) that offered phones at no cost are to be included by the Master Agreements awarded by this solicitation if the Contractor is awarded under this solicitation. For any new plans offered under this contract, Proposers have the flexibility to include a subsidized phone in the plan cost or to require the user to provide a device or pay for it separately.

Financing

Financing is allowed under the Master Agreement, but may be subject to each PA as some jurisdictions may not allow Financing.

Individual Responsible (IRU) Plan Discount

Pricing Discounts for Individual Responsible plans by public employees are to be stated on the Cost sheet. See Section 5.

Waiver of Service Activation Fees

Service Activations Fees will not be allowed under the Master Agreements that derive from this solicitation.

Number Porting

Carrier must provide wired or wireless number porting to/from the mobile device with no charges or penalty.

Upgrade

Users must be able to upgrade or downgrade their service plan at any time with no limits and no restarting of service line contract terms.

Cancellation Fees

Carrier must provide for any participating entity the ability to cancel at least 25% of the active lines of service under contract (subsidized device) in any given year with no early termination fees or other cancellation fees.

Carrier must not assess any cancellation fee or early termination fee for any lines of service that are provided under a Bring Your Own Device option where subsidized equipment is not included in the monthly rate plan cost.

Activation and Billing

Carrier must not commence billing for a device until completion of an order and activation request is executed by the participating entity representative, the user or another individual designated by the participating entity representative. Specific billing and activation procedures may be refined within Participating Addenda.

Cost Sheet

Contractor must populate the cost sheet Attachment C. The plans identified in Attachment C are to be offered to end users and will be included in Attachment G. Contractor must also indicate a discount for plans available under the master agreement that results from this solicitation., that are not entered into Attachment C.

Plan Description

Contractor must include detailed descriptions of all new rate plans approved by the lead state by fully populating Attachment G with complete details related to each plan and feature offered under this contract.

Presentation

Contractors should propose plans that can be easily understood without complex restrictions and terms. Scoring will reflect the degree of concise and impactful plans – from flexibility and cost perspectives.

2.1.7 Internet of Things (IoT) Services

Data plans related to Internet of Things services are covered by this award category. Please describe your Internet of Things offering as it relates to Attachment L, Network Technology Questionnaire in your proposal.

2.1.8 Public Safety/Wireless Priority Service

2.1.8 PUBLIC SAFETY CATEGORY

The Wireless Services Provider (Contractor) will describe how their proposal if and how they intend to provide an exclusive, dedicated broadband network for public safety communications to public safety entities and first responders.

Contractor will describe if and how they would provide for a dedicated network exclusive for use by emergency response providers such as Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities; including Native American Tribes (Sovereign Nations) or authorized tribal organization and rural communities, unincorporated town or village, or other public entity.

Carriers will describe how their proposed services will have the ability to provide the most comprehensive, reliable coverage and highest priority for emergency communications, such as:

- Broadband LTE network allowing first responders and other public safety personnel to send and receive voice, data, video, images, push-to-talk and text without concerns about network congestion.
- Mobile Devices
- Mobile Device Management, to include Maintenance and Replacement
- Public Safety Applications and Solutions
- Assured Priority and Preemption when needed
- Network Security

Interoperability:
Interoperability is critical to all public safety agencies, therefore; The Wireless Service Provider (the Contractor), will describe how they enable comprehensive public safety broadband interoperability at all levels including the sharing of priority and preemption protocols, applications, and mission critical Push-to-Talk (MCPTT) communications and off-air device to device communications during an emergency situation.

Deployable Access:
The Wireless Service Provider (the Contractor) will describe how they will provide cellular connection in areas where service does not exist or where service fails during emergency circumstances. The Wireless Service Provider will describe how they provide dedicated access to Satellite Cell on Wheels and Portable Emergency Communications.

The Wireless Service Provider (Contractor) will describe additional deployable equipment for dedicated access in areas where service does not exist or where service fails during emergency situations.

Optional Services:
Additional Public Safety Services sold under the NASPO ValuePoint Master Agreement other than the requirements listed, must be properly reviewed and approved by the lead state.

Option to Terminate:
The NASPO ValuePoint Master Agreement is an additional procuring mechanism. The Wireless Service Provider (the Contractor) must agree; if a Public Service Entity chooses to utilize the

NASPO ValuePoint Master Agreement, the procuring agency has the option to terminate their agreement at any time without added fees or penalties for cancellation.

The Lead State may cancel the Public Safety/Wireless Priority Service portion of the Category 1 Scope at any time. If the Lead State chooses to cancel the Public Safety/Wireless Priority Service portion of Category 1 Scope, it will provide contractors with 180 days notice.

No other Terms and Conditions, End User Agreements, or any other terms will be offered with the new product or service unless it is included in the Master Agreement.

2.2 Category 2- Equipment and Accessories

This category includes any equipment or accessories operating over cellular carrier provided network services or intended for use with cellular connected devices.

This Award Category is for National Award only.

2.2.1 Definitions

Accessories Any equipment, component or add-on accessory intended for use with cellular connected devices.

Equipment Any device operating over cellular carrier provided network. Does not include servers, desktops or laptop computing devices.

Cellular Devices Any phones or other equipment used to connect over wireless services offered by cellular carriers (Category 1).

2.2.2 Eligible Equipment and Accessories

Those products eligible as equipment and accessories under this solicitation, currently includes and may be expanded as technology advances:

- Basic Cellular Devices
- Smartphones - iOS, Android, Other
- Stand Alone, Integrated or USB Dongle Cellular Modems
- Wi-Fi/Cellular Routers
- Tablets that are cellular-network connected
- Other equipment with a primary purpose for communicating over the cellular carrier network, currently including:
  - Sensors

    - Cellular-enabled Video cameras
- Accessories:
    - Replacement Batteries
    - Cases & related accessories
    - Screen Protectors
    - Chargers
    - Cords / cables
    - Signal Boosters / antennae
    - Headsets and speakers for use with wireless devices

2.2.3 Service Requirements

Condition of Equipment and Accessories

All equipment and accessories provided under this contact must be new, unused and properly functioning when received by participating entity if priced as a new product.

Superseded, used, returned, or reconditioned items will be accepted if labelled as such in the sales order.

Trial Period

Contractor may allow for a designated trial period for testing/evaluating equipment and accessories without additional charges or fees if applicable. Contractor will describe the timeframe for the 'trial period' and procedures for implementing this policy in the sales invoice or purchase order.

Return of Equipment and Accessories

Any equipment or accessories that are not properly functioning when received by the participating entity must be replaced by the contractor with new and properly functioning equipment or accessories within 5 business days of the defective equipment or accessories being reported to the contractor.

Participating entities shall not be responsible for any costs related to the return and/ or replacement of any equipment or accessories that are returned due to quality problems, duplicate shipments or other shipping errors, outdated products or other issues related to non-compliance with terms of this agreement. Contractors must confirm in writing to the end user when returns are received.

Participating entities shall not be assessed restocking fees or any other fees for items trialed and then returned as unacceptable for any reason.

Contractor will allow for equipment and accessory purchases at all retail stores open to the public. Sales personnel at retail stores will be aware of pricing from the Master Agreement that results from this solicitation.

2.2.4 Pricing

Cost Sheet

See Attachment C for details for Award Category 2.

Financing

Financing is allowed under the Master Agreement, but may be subject to each PA as some jurisdictions may not allow Financing.

Individual Responsible (IRU) Plan Discount

Pricing Discounts for equipment and accessories offered to public employees with Individual Responsible plans are to be stated on the Cost sheet (Attachment C). See section 5 for additional details.

Shipping
Contractor if a Carrier must activate service on new equipment within 72 hours of request or shipping.

2.3 Category 3 – Internet of Things and other Turnkey Wireless Applications

This category includes any of the wireless or IoT solutions or applications being offered as a complete product by the cellular wireless carriers or any other Contractor(s).

This Award Category may be for National Award, or Regional Award at the indication of the Contractor in their proposal. Contractors will indicate this preference in Attachment W.

Awards will be made in each individual sub-category of Category 3, not for Category 3 as a whole. An award in one sub-category does not entitle a vendor to offer products or services in any other subcategories for which they were not specifically awarded.

2.3.1 Definitions

Turnkey Wireless Solution For the purposes of this solicitation a Turnkey Wireless Solution is an integrated, on premise or hybrid system that includes three broad elements:

- End Points physical objects (things like sensors, cameras, end point devices, etc.) that contain embedded technology to sense or interact with their internal state or external environment and the ability to communicate with a remote application
- Network Services a wireless communication network providing M2M communication services or some other method of data transport connecting the dedicated physical objects with;
- Back Office Systems applications and central or back end systems (servers, software, operating systems, storage, etc.).

2.3.2 Turnkey Wireless Solutions

A Proposal shall fully disclose what is included in the Turnkey Wireless Solutions, including all operational components, training, services, equipment, licenses, third party agreements, any and all fees and performance guarantees.

Products and services offered by carriers/Contractors under Legacy Plans that are now part of Category 3 awards under this solicitation will be part of the contracts that result from this solicitation if the carrier/Contractors has also been awarded under that Category and Sub-category.

For example: MDM products under legacy plans may only be offered under the new Master Agreement if the Contractor is awarded under the MDM subcategory of Category 3 awards.

If an Contractor is not awarded a product under an Award Category 3 subcategory, but has provided a product or service under Legacy Plans, the Contractor may continue to offer the product to end users already under contract. The product may not be offered to new end users unless the Contractor has won award of the subcategory.

<u>Turnkey Wireless Solutions Single Contract</u> The provider offering a Turnkey Wireless Solutions may utilize subcontractors and partners to provide various elements of the system, but the system including all licensing rights will be covered by a single contract between the end user that purchases the system and the provider who is awarded a master agreement for this category of award.

<u>Limited Related Service</u> The provider shall provide support services as needed to install, maintain and enhance the system over the life of the system. These Limited Related Services shall be included in the system pricing. Installation services may be capped in proportion to the project at hand. The Proposal shall describe all related services that are included in the Turnkey Wireless System. The purchasing entity shall have the option to purchase additional services at pricing offered by the proposer and provide an hourly rate related to the project for the Additional Consulting or Integration Services.

<u>Additional Consulting or Integration Services</u>

a. The purchasing entity shall have the ability to purchase consulting or integration services from the provider.
b. Consulting Services – In Category 3, “Consulting Service” means planning, assessment and other professional consulting services provided by the Contractor related to the public entities planning, design, assessing, operating or maintaining an IoT solution.
c. Additional Services – In Category 3, “Integration Service” means the process of making new IoT devices, data, platforms and applications, as well as existing IT assets (for example, business applications, data, mobile, SaaS and legacy systems) work well together in the context of implementing end-to-end IoT business solutions. Integration services are not part of turnkey system or limited related service, but may be acquired from the provider or from a separate integration service provider at the sole discretion of the purchasing entity.

Limited Related Service and Additional Consulting or Integration Services will be billed at an Hourly rate will be included on the Cost Sheet (Attachment C) and will be included in the Master Agreement. The Hourly rate will be a blended rate and will encompass all related cost for these additional services.

2.3.3 Category 3 Subcategories of Award

See Attachment V for Category 3 Subcategory Definitions.

<u>Right to Refresh</u>

This category of master agreements (Turnkey Wireless Solutions) may be reopened and refreshed at the sole discretion of the Lead State at any time. The refresh may allow additional Turnkey Wireless Solutions offering in the broad scope or by specifically identified sub categories. The

Lead State reserves the right to change the methodology for award for all or any subcategories at the time of the refresh/reopen of the solicitation. Awards for Award Category 3 in any refresh solicitation will be given the same contract term as the initial award.

Data Protection

The provider shall:

a. Specify the best available standards-based encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.
b. Describe whether or not it is willing to sign relevant and applicable agreements that may be necessary to protect data with a Purchasing Entity.
c. Describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement.
d. Specify its data disposal procedures, policies and destruction confirmation process

Subcontractors
Providers must explain for each Turnkey Wireless Solutions offered if they intend to provide it directly or through the use of Subcontractors. Any Subcontractor that a Provider chooses to use in fulfilling the requirements of the solicitation must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the solutions provided in this category.

a. Contractor must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.
b. If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP.
c. Include a description of how the Contractor will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

2.3.4 Security For each Turnkey Wireless Solutions proposed include both a security disclosure statement.

Contractors for Award Category 3 must submit answers to Attachment S.

2.3.5 Client Infrastructure Impact and Support

Contractors will be willing to provide a description of the Impact and Support on End User infrastructure upon request Assessment what impacts the Turnkey Wireless application will have on the infrastructure used by purchasing entity, including the client's network, data storage and client owned and operated endpoints before installation. Contractor will at the time of purchase identify any support required by the purchasing entity to support the proposed Turnkey Wireless Solutions.

2.3.6 Client Infrastructure and Support

Unless the purchasing entity waives the requirement, the Contractor shall provide a description of the Impact and Support on the End User infrastructure. This shall include an assessment of impacts the Turnkey Wireless application will have on the infrastructure used by purchasing entity, including the client's network, data storage and client owned and operated endpoints before installation. The description shall also identify any resources required by the purchasing entity to support the proposed Turnkey Wireless Solutions.

2.3.7 Pricing Requirements

Cost Sheet

See Attachment C for details for Award Category 3.

No other Terms and Conditions, End User Agreements, or any other terms will be offered with the new product or service unless it is included in the Master Agreement at formation or by Amendment.

Section 3: Adding New Products and Services

The Lead State anticipates establishing a process for regular communication with contractors and addition of new products and services. Addition of new products will be treated differently based on which category of award covers the product or service.

3.1 General Requirements

The Lead State, along with the sourcing committee of this Solicitation will review and add new products and services to the Master Agreements outlined below. The Lead State reserves the right to modify this process to ensure open, transparent and reasonable review of proposed new products and services.

3.2 New Products added under Award Category 1

For new service plans under Award Category 1, Carriers may add new plans as they become available to end users, so long as the plans are added to Attachment G, Contract Coverage Attachment, at the next quarterly update and therefore incorporated into the Master Agreement. If the new plans are not added to Attachment G at the next quarterly update, they will not be included within the scope of the Master Agreements that result from this solicitation. Once plans are incorporated into the Master Agreement in this manner, they are subject to the termination restrictions in section 2.1.4.

3.3 New Products added under Award Category 2

Contractors may add new products under Award Category 2 at any time as long as they fall within the scope of that award category. The Lead State reserves the right to make the determination of whether a product falls within award category 2.

3.4 New Products added under Award Category 3

For new products under Award Category 3, Contractors must submit a request to the Lead State and sourcing team for consideration using Attachment N. All new products under Award Category 3 will be allowed only through amendment of the Master Agreements that result from this solicitation.

After consultation with the sourcing team, the Lead State may choose to include the new product under the Master Agreements by amendment. The Contractor will provide an updated Attachment G at the next quarterly update for public distribution.

3.4.1 New Product Request Form

The New Product Request form will be submitted to the Lead State to request any new products or services under Award Category 3(See Attachment M).

Proposed additional terms and conditions, end user agreements or related materials to be used with the new product must be included with the New Product Request form to be considered for addition to the Master Agreement. Terms and Conditions for additional products/services may be negotiated by the Lead State before addition.

3.4.2 New Product Request Log

All new added products and services under Award Category 3 will be included on Attachment N, Request Log sheet that will include Lead State recommendations and observations. This log will be included in the contract file and will be available for public view.

3.4.3 Quarterly Amendments

The Lead State expects to conduct quarterly amendments of the Master Agreement to add new products and services under Award Category 3. The Lead State reserves the right to amend, or not amend the Master Agreement at any time.

Terms and Conditions not included in the addition of new products for Award Category 3 will not be part of any agreement with end users. Contractors will present end users only with the Terms and Conditions agreed to by the parties in the Master Agreement Amendment.

3.4.4 Terms and Conditions Compliance with Master Agreement

All Products offered under Award Category 3 shall comply fully with all applicable Federal and State laws and regulations. The Order of Precedence clause in the NASPO ValuePoint Master Agreement Terms and Conditions and/or Participating Addendum will control in the event of any conflict between the NASPO ValuePoint Master Agreement and/or Participating Addendum and the Product Terms and Conditions. Any third-party product provider must agree to the Master Agreement Terms and Conditions.

3.5 Quarterly Call/Meeting

The Lead State expects to have a call with contractors every quarter to discuss the status of the contracts, discuss proposed new products and services, and any other issues that may arise regarding the contract. These calls/meetings will be scheduled at mutually agreed upon times.

3.6 Terms and Conditions Compliance with Master Agreement

Any and all Products offered and furnished under any award category shall comply fully with all applicable Federal and State laws and regulations. The Order of Precedence clause in the NASPO ValuePoint Master Agreement Terms and Conditions and/or Participating Addendum will control in the event of any conflict between the NASPO ValuePoint Master Agreement and/or Participating Addendum and the Product Terms and Conditions. Any third-party product provider must agree to the Master Agreement Terms and Conditions.

Section 4: Individual Responsible Account Discounts

4.1 Individual Responsible Account Definition

Individual Responsible Accounts ("IRU") are accounts for products and services between Contractors awarded a contract under this solicitation and individuals who are employees of eligible users of the Master Agreement. IRU accounts are for the personal use of individual employees of eligible end users of the Master Agreement. IRU discount offerings are not required by Contractors but are scored as a Technical Scorable Criteria for Award Category 1.

All other plans used under this contract by eligible end users are Government/Corporate Responsible Plans (CRU).45.2 Corporate Responsible Account Definition

Corporate Responsible Accounts ("CRU") are accounts for end users of the Master Agreement.

4.3 Discount for Individual Responsible Account offerings

Contractors will indicate what, if any discount they allow for IRU accounts under this Master Agreement. This discount is entered in their Costsheet (Attachment C) and be included in the Master Agreement.

Section 5: Reporting

5.1 General Requirements

5.1.1 Reporting shall be provided in the format required by NASPO ValuePoint:

6.1.1.1 Attachment H (Award Category 1)

6.1.1.2 Attachment I (Award Category 2)

6.1.1.3 Attachment J (Award Category 3)

5.1.2 Attachment G: Contract Coverage Attachment

Contractors under the Master Agreement that results from this contract will submit quarterly Attachment G to the Lead State. This attachment is intended to encapsulate the plans, services and offerings of the contractor. This would include any legacy and current offerings, including the plans entered on Attachment C. (anything that would be covered by the Master Agreement).

For Award Category 1, all legacy plans that have a discount under the Current Nevada Master Agreement must continue the discount to be covered by the Master Agreement that results from this solicitation. All legacy plans that do not have a discount under the Current Nevada Master Agreement may continue to have no discount under the Master Agreement that results from this solicitation

Attachment G must be submitted by Contractors awarded under Award Category 1, Award Category 3 and Award Category 4.

5.1.3 Individual participating entities may request specific equipment sales summaries, which shall be provided at no cost.

Upon request, provide reporting elements and/or management reports related to usage for services that are available and would optimize the participating entity's ability to assess utilization and cost.

Be able to provide custom reports as may be requested by individual participating entities. Describe in general, the level of sophistication and complexity, custom usage report data that you can provide to the participating entities. Vendors should provide a sample report with their proposal.

Upon request, provide subscribers with usage reports which include full itemization of call details (such as the information on the Contractor's standard bill for consumer accounts) to enable verification of usage including: (1) call date, call number call length, call time, and (2) plan cost, per minute charges, overage cost, additional features charges and other fees, etc.

5.2 Quarterly Call/Meeting

Contractors must be available for a quarterly meeting by phone, video conference, or in person to discuss contract concerns, developments and any upcoming additional products or services related to reporting.

5.4 Usage Reports (Other States)

Other States and participating entities may have alternate reporting requirements and will be addressed by their Participating Addendum.

Section 6: Pricing Landing Page

6.1 General

NASPO ValuePoint will develop a pricing landing page (webpage) to display contractor pricing in several key areas on an ongoing basis. It is anticipated that the end users will be able to use this Pricing Landing page as a tool to aid in pricing and negotiating plans and device accessory purchases from all awarded contractors. Contractors are expected to provide certain required fields for the Pricing Landing Page. This Section applies only to Category 1 awards.

6.2 Pricing Landing Page Requirements

6.2.1 General Requirements

The Pricing Landing Page will consist of a webpage to allow for quick reference of plans, equipment, accessories and services offered by contractors. Contractors may update the required fields at their discretion whenever they wish. The fields must be populated by contractors.

6.2.2 for Carriers/Contractors (Awarded under Category 1)

At the onset of the contract, Carriers/Contractors will be required to enter in pricing plans for the following scenarios that are found in Attachment C (Costsheet):

- Plans that include a subsidized device in the monthly rate plan cost
    - Basic phone with unlimited voice and messaging
    - Smartphone - 4 Gig of data, unlimited voice & messaging
    - Smartphone - 300 minutes of voice, unlimited data & messaging
    - Smartphone - unlimited data, voice & messaging
    - data only - low - 150 kb
    - data only - moderate - 4 Gig
    - data only - unlimited data
- Plans that require user to supply the device or pay for it separately
    - Smartphone - 4 Gig of data, unlimited voice & messaging
    - Smartphone - unlimited data, voice & messaging
    - Tablet - 1 Gig of data
    - Tablet - shares data with other devices
    - data only - low - 150 kb
    - data only - moderate - 4 Gig
    - data only - unlimited data

These categories have been identified as representing the rate plans and services that are most commonly purchased by NASPO Participating Entities. The categories may be changed as desired by the contractor by submitting updates to NASPO ValuePoint.

6.3 Pricing Landing Page Features

Pricing information

The Lead state will develop a required reporting based on the 14 scenarios listed in Attachment C for the landing page. The lead state reserves the right to determine requirements.

Disclaimers

Clear disclaimers to end users that all pricing reflects contractors best estimates for hypothetical use cases and does not represent local fees, taxes and potential discounts available at specific locations

Point of Contact Information

Sales, Customer Service and Contract Administration point of contact information for ease of reference

Current Offers

Current Discounts, Offers, and Specials available to end users. This would be done on a national basis. Disclaimers for reasonable variance will be allowed at the discretion of the lead state.

Section 7: Administration of Contracts

7.1 Quarterly Amendment

The Lead State anticipates it will provide for regular quarterly amendments to the Master Agreement if there is a need to add new products or services. (Section 4). The Lead State at its discretion may elect to amend the Master Agreement at any time.

7.2 Quarterly Call

The Lead State and sourcing team intend to hold quarterly calls to facilitate new products/services, discuss the administration of the Master Agreements, and all other applicable aspects of the master agreement.

7.3 Annual Meeting

Contractors must be available for an annual meeting in person to discuss continuing administration of the contract. The Lead State anticipates meeting once a year in person to facilitate more in depth communication. The location of in-person meetings will be in The Salt Lake City area, or elsewhere at the discretion of the Lead State.

7.4 Published Documents

The Lead State intends to publish all new product/service request forms, new product logs, and any sourcing committee recommendations and notes related for reference. End users may use these documents to aid in their purchasing decisions.

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 1 Costsheet

Vendor Name: Sprint

Subsidized Device Scenarios						***Bring Your Own Device Scenarios***					
Scenario	***Description*** *carrier provides a device along with the rate plan. Pricing is for 1 device/plan as applicable per scenario.*	***rate ($ per month)***	***Usage Weight***	***Weighted Cost***	***OFFEROR NOTES*** Describe plan attributes and characteristics per the instructions*.	***Scenario***	***Description*** *assume customer provides own device separately. Pricing is for 1 device/plan as applicable for scenario.*	***rate***	***Usage Weight***	***Weighted Cost***	***OFFEROR NOTES*** Describe plan attributes and characteristics per the instructions*.
1	basic phone - unlimited voice & messaging	$19.99	0.115	$2.30	**PS Unlimited Feature Phone Plan**: Unlimited Anytime Minutes, Unlimited messages, Sprint Mobile to Mobile. Includes Direct Connect Plus, Nationwide LD, and Caller ID & Voicemail.	8	Smartphone - 4 Gig of data, unlimited voice & messaging	$25.00	0.01	$0.25	**Sprint Plan for Unsubsidized Device UNLIMITED**: Includes Unlimited Anytime Minutes, Unlimited Messages, Unlimited Data, 10GB mobile hotspot, 100MB of Data roaming (Data roaming overage rate = $0.25/MB). Plan is for Unsubsidized devices only.
2	Smartphone - 4 Gig of data, unlimited voice & messaging	$39.99	0.055	$2.20	**Sprint Public Sector All In Smartphone – Green**: Unlimited Anytime Minutes, Unlimited Messages, Includes Voice Roaming, Caller ID & Voicemail, Unlimited Internet browsing and email, Data Roaming, and Premium Data.	9	Smartphone - unlimited data, voice & messaging	$25.00	0.01	$0.25	**Sprint Plan for Unsubsidized Device UNLIMITED**: Includes Unlimited Anytime Minutes, Unlimited Messages, Unlimited Data, 10GB mobile hotspot, 100MB of Data roaming (Data roaming overage rate = $0.25/MB). Plan is for Unsubsidized devices only.
3	Smartphone - 300 minutes of voice, unlimited data & messaging	$39.99	0.357	$14.28	**Sprint Public Sector All In Smartphone – Green**: Unlimited Anytime Minutes, Unlimited Messages, Includes Voice Roaming, Caller ID & Voicemail, Unlimited Internet browsing and email, Data Roaming, and Premium Data.	10	Tablet - 1 Gig of data	$15.00	0.01	$0.15	**Business Share Plus for Phones, Tablets, MBB, IoT, M2M** - 1GB Plan. Pricing provided is for current customers. For New Customers, the MRC is $12.75.
4	Smartphone - unlimited data, voice & messaging	$39.99	0.048	$1.92	**Sprint Public Sector All In Smartphone – Green**: Unlimited Anytime Minutes, Unlimited Messages, Includes Voice Roaming, Caller ID & Voicemail, Unlimited Internet browsing and email, Data Roaming, and Premium Data.	11	Unlimited Data Plans (no Throttling) that are used by First Responders	$22.99	0.01	$0.23	**3G/4G Connection Card Plan Charges – BYOD**: Unlimited for Acceptable Use, 100MB of Data roaming (Data roaming overage rate = $0.25/MB)
5	data only - low - 150 kb	$1.00	0.014	$0.01	**Sprint Data Rate Plans:** 150KB Data	12	data only - low - 150 kb	$1.00	0.01	$0.01	**Sprint Data Rate Plans:** 150KB Data
6	data only - moderate - 4 Gig	$30.00	0.04	$1.20	**Business Share Plus for Phones, Tablets, MBB, IoT, M2M** - 4GB Plan. Pricing provided is for current customers. For New Customers, the MRC is $25.50.	13	data only - moderate - 4 Gig	$18.99	0.01	$0.19	**Sprint Data Rate Plans:** 4GB Data
7	data only - unlimited data	$29.99	0.287	$8.61	**3G/4G Connection Plan**: Unlimited for Acceptable Use, 100MB of Data roaming (Data roaming overage rate = $0.25/MB)	14	data only - unlimited data	$29.99	0.01	$0.30	**Embedded Computing Connection and Router Plan** Unlimited for Acceptable Use, 100MB of Data roaming (Data roaming overage rate = $0.25/MB)
Total				$30.52		Total				$1.38	
Grand Total (C14 + K14)				$31.90							

Subsidized Device Scenario Requirements			***Bring Your Own Device Scenarios***		
Scenario	***Description***	***requirements***	***Scenario***	***Description***	***requirements***
1	basic phone - unlimited voice & messaging	*monthly rate covers 1 user / plan for device, network access, unlimited voice talk time and unlimited messaging *device must be most current in stock device *data used on device will be pulled from account pool *plan includes unlimited messaging from the US to other countries	8	Smartphone - 4 Gig of data, unlimited voice & messaging	*monthly rate covers 1 user / plan for network access, unlimited voice talk time, unlimited messaging, unlimited mobile hot spot and at least 4 Gig of 4G data *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance *plan includes unlimited messaging from the US to other countries
2	Smartphone - 4 Gig of data, unlimited voice & messaging	*monthly rate covers 1 user / plan for device, network access, unlimited voice talk time, unlimited messaging, unlimited mobile hot spot and at least 4 Gig of 4G data *device must be no older than one generation removed from most current model *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance *plan includes unlimited messaging from the US to other countries	9	Smartphone - unlimited data, voice & messaging	*monthly rate covers 1 user / pland for network access, unlimited voice talk time, unlimited messaging, unlimited mobile hot spot and unlimited 4G data *data must not throttle before at least 20 gigs of data have been used in the current month *plan includes unlimited messaging from the US to other countries
3	Smartphone - 300 minutes of voice, unlimited data & messaging	*monthly rate covers 1 user / plan for device, network access, 300 minutes of voice talk time, unlimited messaging, unlimited mobile hot spot and unlimited 4G data *device must be no older than one generation removed from most current model *data must not throttle before at least 20 gigs of data have been used in the current month *minutes must contribute to overall account pool *plan includes unlimited messaging from the US to other countrie:	10	Tablet - 1 Gig of data	*monthly rate covers 1 user / plan for network access, unlimited mobile hot spot and at least 1 Gig of 4G data *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance
4	Smartphone - unlimited data, voice & messaging	*monthly rate covers 1 user / plan for device, network access, unlimited voice talk time, unlimited messaging, unlimited mobile hot spot and unlimited 4G data *device must be no older than one generation removed from most current model *data must not throttle before at least 20 gigs of data have been used in the current month *plan includes unlimited messaging from the US to other countries	11	Unlimited Data Plans (no Throttling) that are used by First Responders	*monthly rate covers 1 user / pland for network access, unlimited voice talk time, unlimited messaging, unlimited mobile hot spot and unlimited 4G data *plan includes unlimited messaging from the US to other countries
5	data only - low - 150 kb	*monthly rate covers 1 user / plan for device, network access and at least 150 kb of 4G data *device must be no older than one generation removed from most current model *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance	12	data only - low - 150 kb	*monthly rate covers 1 user / plan for network access, at least 150 kb of 4G data *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance
6	data only - moderate - 4 Gig	*monthly rate covers 1 user / plan for device, network access, at least 4 Gig of 4G data and unlimited mobile hotspot *device must be no older than one generation removed from most current model *data must contribute to overall account pool	13	data only - moderate - 4 Gig	*monthly rate covers 1 user / plan for network access and at least 4 Gig of 4G data and unlimited mobile hotspot *data must contribute to overall account pool *unused data from the previous month may roll over into the next month's allowance
7	data only - unlimited data	*monthly rate covers 1 user / plan for device, network access, unlimited 4G data and unlimited mobile hotspot *device must be no older than one generation removed from most current model *data must not throttle before at least 20 gigs of data have been used in the current month	14	data only - unlimited data	*monthly rate covers 1 user / plan for network access, unlimited 4G data and unlimited mobile hotspot *data must not throttle before at least 20 gigs of date have been used in the current month

Catalog Discount Offering

Descripiton	***Pecentage Off (%)***	***What aspects of plans does this discount apply to? Please be specific.***
Percentage off discount rate offered plans as defined by the Scope of Work (Must be an entry to be responsive)	25.00%	Discount off eligible plans. Plans proposed above are Custom and NET no discounts apply.

ILU Discount Offering

Descripiton	***Pecentage Off (%)***	***What aspects of plans does this discount apply to? Please be specific.***
Percentage off discount rate offered to ILU accounts as defined by the Scope of Work	19.00%	The Employee Discount may be in the form of a fixed dollar consumer rate plan discount, a gift card or other similar offer, or an 19% discount applied to eligible Sprint consumer rate plans before taxes and surcharges.

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 2 Costsheet

Vendor Name: Sprint

Item Number	Item Description	Manufacture/Brand	Model	Price Per Unit	MSRP	Category Percentage off of MSRP (If applicable)	Average Cost	Notes
1	Cases	Otterbox	Symmetry Series Case - Apple iPhone 7/8	$29.99	$39.99	25.00%	$23.74	Additional Accessories available upon request
		Incipio	Incipio NGP Case - iPhone 7/6/6s	$18.74	$24.99	25.00%		Additional Accessories available upon request
		Brightstar/ OffWire	Sonim Holster with Swivel Clip for XP5s	$22.49	$29.99	25.00%		Additional Accessories available upon request
2	Screen Protectors	Ash Cloud	Key Liquid Screen Protection	$33.74	$44.99	25.00%	$28.74	Additional Accessories available upon request
		Brightstar/ OffWire	Key Tempered Glass Screen - LG Tribute Dynasty	$22.49	$29.99	25.00%		Additional Accessories available upon request
		ZAGG/iFrogz	InvisibileSHIELD GLASS Screen - LG X power	$29.99	$39.99	25.00%		Additional Accessories available upon request
3	Chargers	Brightstar/ OffWire	KEY 3.4 Amp Dual Port Wall Charger	$11.24	$14.99	25.00%	$14.99	Additional Accessories available upon request
		Brightstar/ OffWire	KEY 4.8A Dual USB Car Charger	$18.74	$24.99	25.00%		Additional Accessories available upon request
		Brightstar/ OffWire	KEY Quick Charge 3.0 Wall 1 Port	$14.99	$19.99	25.00%		Additional Accessories available upon request
4	Headsets for use with wireless devices	Apple	Apple EarPods with Lightning Connector	$22.49	$29.99	25.00%	$47.49	Additional Accessories available upon request
		LG	LG TONE PRO (HBS-780) Bluetooth Stereo Headset - Gold	$59.99	$79.99	25.00%		Additional Accessories available upon request
		Samsung	Samsung U Flex Headphones - Ivory	$59.99	$79.99	25.00%		Additional Accessories available upon request
5	Speakers for use with wireless devices	Harman International	JBL Clip 3 Portable Speaker - Black	$44.99	$59.99	25.00%	$44.99	Additional Accessories available upon request
6	Basic Cell Phone	Alcatel	Alcatel Dawn	$0.00	$96.00	0.00%	$0.66	Additional Devices available upon request
		Sonim	Sonim XP Strike (XP3410)	$0.99	$329.99	0.00%		Additional Devices available upon request
		Sonim	Sonim XP Strike IS (XP3420)	$0.99	$329.99	0.00%		Additional Devices available upon request
7	Push to Talk Device	Kyocera	Kyocera DuraXTP	$49.99	$270.00	0.00%	$83.32	Additional Devices available upon request
		Kyocera	Kyocera DuraForce Pro (3GB)	$99.99	$432.00	0.00%		Additional Devices available upon request
		Kyocera	Kyocera DuraTR	$99.99	$324.00	0.00%		Additional Devices available upon request
8	SmartPhones	Apple	iPhone 6S (32GB)	$0.00	$449.99	0.00%	$16.66	Additional Devices available upon request
		Apple	iPhone 7 (32GB)	$0.00	$449.99	0.00%		Additional Devices available upon request
		Samsung	Samsung Galaxy J7 Perx	$49.99	$270.00	0.00%		Additional Devices available upon request
9	Tablets	Apple	iPad (32GB) (6th gen)	$359.99	$459.99	0.00%	$169.99	Additional Devices available upon request
		LG	LG G Pad F2 8.0	$49.99	$149.99	0.00%		Additional Devices available upon request
		Samsung	Samsung Galaxy Tab E	$99.99	$199.99	0.00%		Additional Devices available upon request
10	Cellular Modems stand alone, integrated or USB	Franklin	Franklin U772 USB Modem	$19.99	$180.00		$19.99	Additional Devices available upon request
11	MiFi Hot Spots	Franklin	Franklin R850 Mobile Hotspot	$0.00	$144.00		$0.00	Additional Devices available upon request
		ZTE	ZTE Warp Connect Hotspot	$0.00	$144.00			Additional Devices available upon request
12	WiFi Cellular Routers			$0.00			$0.00	Not Applicable
				$0.00				
				$0.00				
13	IoT Sensors			$0.00			$0.00	Not Applicable
				$0.00				
				$0.00				
14	Cellular-enabled video cameras			$0.00			$0.00	Not Applicable
				$0.00				
				$0.00				
15	Cords / cables			$0.00			$0.00	Not Applicable
				$0.00				
				$0.00				
16	Signal Boosters / Antennas			$0.00			$0.00	Not Applicable
				$0.00				
				$0.00				
Total							$159.96	

ILU Discount Offering

Descripiton	Pecentage Off (%)	What aspects of plans does this discount apply to? Please be specific.
Percentage off discount rate offered to ILU accour	19.00%	Applies to eligible discountable plans

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Category 3A: Fleet Management Costsheet

VENDOR		Sprint

Monthly Recurring Cost

Description	***minimum quantity of vehicles***	***monthly fee***	***total annual cost*** *(qty x fee x 12)*	***OFFEROR NOTES*** Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	$15.00	$1,800.00	**Actsoft Fleet Management (primary) Solutions**: Encore Fleet Vehicle (unbundled)
	100	$15.00	$18,000.00	**Actsoft Fleet Management (primary) Solutions**: Encore Fleet Vehicle (unbundled)
	500	$15.00	$90,000.00	**Actsoft Fleet Management (primary) Solutions**: Encore Fleet Vehicle (unbundled)
	1000	$15.00	$180,000.00	**Actsoft Fleet Management (primary) Solutions**: Encore Fleet Vehicle (unbundled)
	5000	$15.00	$900,000.00	**Actsoft Fleet Management (primary) Solutions**: Encore Fleet Vehicle (unbundled)
Total Annual Recurring Cost			**$1,189,800.00**	

Service Requirements

Description		***requirements***
Basic Fleet Management		*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs

Description	***minimum quantity of vehicles***	***cost per vehicle***	***Total Set Up Cost***	***OFFEROR NOTES*** Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	$199.00	$1,990.00	Hardware Charge
	100	$199.00	$19,900.00	Hardware Charge
	500	$199.00	$99,500.00	Hardware Charge
	1000	$199.00	$199,000.00	Hardware Charge
	5000	$199.00	$199,000.00	Hardware Charge
Total Installation and Set Up Cost			**$519,390.00**	

Installation & Set Up Requirements

Description		***requirements***
Installation, Set Up and Basic System Administrator Training		*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost	**$1,709,190.00**

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet				
Category 3A: Fleet Management Costsheet				
VENDOR		Sprint		
Monthly Recurring Cost				
Description	***minimum quantity of vehicles***	***monthly fee***	***total annual cost*** *(qty x fee x 12)*	***OFFEROR NOTES*** Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	$18.00	$2,160.00	**Geotab Basic:** provides features that are GPS position and time-based, including: location, breadcrumb trail, geofencing, idling, speeding, stop/start times and time/location-based safety alerts, and maintenance reminders
	100	$18.00	$21,600.00	**Geotab Basic:** provides features that are GPS position and time-based, including: location, breadcrumb trail, geofencing, idling, speeding, stop/start times and time/location-based safety alerts, and maintenance reminders
	500	$18.00	$108,000.00	**Geotab Basic:** provides features that are GPS position and time-based, including: location, breadcrumb trail, geofencing, idling, speeding, stop/start times and time/location-based safety alerts, and maintenance reminders
	1000	$18.00	$216,000.00	**Geotab Basic:** provides features that are GPS position and time-based, including: location, breadcrumb trail, geofencing, idling, speeding, stop/start times and time/location-based safety alerts, and maintenance reminders
	5000	$18.00	$1,080,000.00	**Geotab Basic:** provides features that are GPS position and time-based, including: location, breadcrumb trail, geofencing, idling, speeding, stop/start times and time/location-based safety alerts, and maintenance reminders
Total Annual Recurring Cost			**$1,427,760.00**	

Service Requirements		
Description		***requirements***
Basic Fleet Management		*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs				
Description	***minimum quantity of vehicles***	***cost per vehicle***	***Total Set Up Cost***	***OFFEROR NOTES*** Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	$59.99	$599.90	Set Up Fee
	100	$59.99	$5,999.00	Set Up Fee
	500	$59.99	$29,995.00	Set Up Fee
	1000	$59.99	$59,990.00	Set Up Fee
	5000	$59.99	$59,990.00	Set Up Fee
Total Installation and Set Up Cost			**$156,573.90**	

Installation & Set Up Requirements		
Description		***requirements***
Installation, Set Up and Basic System Administrator Training		*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost	**$1,584,333.90**

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Category 3A: Fleet Management Costsheet

VENDOR		Sprint

Monthly Recurring Cost

Description	***minimum quantity of vehicles***	***monthly fee***	***total annual cost*** *(qty x fee x 12)*	***OFFEROR NOTES*** Describe plan attributes and characteristics per the instructions*.
Basic Fleet Management	10	$15.00	$1,800.00	**SPIREON FLEETLOCATE FLEET MANAGEMENT BASIC SOLUTION - UNBUNDLED DATA:** Includes Spireon Web-Based Software
	100	$15.00	$18,000.00	**SPIREON FLEETLOCATE FLEET MANAGEMENT BASIC SOLUTION - UNBUNDLED DATA:** Includes Spireon Web-Based Software
	500	$15.00	$90,000.00	**SPIREON FLEETLOCATE FLEET MANAGEMENT BASIC SOLUTION - UNBUNDLED DATA:** Includes Spireon Web-Based Software
	1000	$15.00	$180,000.00	**SPIREON FLEETLOCATE FLEET MANAGEMENT BASIC SOLUTION - UNBUNDLED DATA:** Includes Spireon Web-Based Software
	5000	$15.00	$900,000.00	**SPIREON FLEETLOCATE FLEET MANAGEMENT BASIC SOLUTION - UNBUNDLED DATA:** Includes Spireon Web-Based Software
Total Annual Recurring Cost			**$1,189,800.00**	

Service Requirements

Description		***requirements***
Basic Fleet Management		*Solution to track, monitor & dispatch vehicles while collecting information on vehicle location & operation *must have option to connect to vehicle's On Board Diagnostic-II (OBD-II) port *Ability to monitor vehicle location *Provide location-based vehicle dispatch support *Collect information on driver performance *Real time and historical reporting via secure, centralized portal *Ability to set up alerts based on customer devined parameters

Installation & Set Up Costs

Description	***minimum quantity of vehicles***	***cost per vehicle***	***Total Set Up Cost***	***OFFEROR NOTES*** Details of Installation and Set Up of customer's instance
Total One Time Cost for Installation, Set Up and Basic System Administrator Training	10	$59.99	$599.90	Set Up Fee
	100	$59.99	$5,999.00	Set Up Fee
	500	$59.99	$29,995.00	Set Up Fee
	1000	$59.99	$59,990.00	Set Up Fee
	5000	$59.99	$59,990.00	Set Up Fee
Total Installation and Set Up Cost			**$156,573.90**	

Installation & Set Up Requirements

Description		***requirements***
Installation, Set Up and Basic System Administrator Training		*Set up and configuration of customer's instance in provider's hosted environment. *install each device in vehicle and connect to OBD-II

Scorable Cost	**$1,346,373.90**

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3F Costsheet

Vendor Name: Sprint

	Product Name	***Product Description***	***Characteristics of Product***	***Percentage Off Discount (%)****	***Notes***
	Canvas Startup - Monthly	Per User; 5 user maximum enforced		5.00%	Discount of MRC
	Canvas Business - Monthly	Per User			Discount of MRC
	Canvas Professional – Monthly	Per User			Discount of MRC
	Canvas Connect – Monthly (1-10 users)	Up to 10 Users			Discount of MRC
	Canvas Connect – Monthly (11-50 users)	For 11 -50 Users			Discount of MRC
	Canvas Connect – Monthly (51+ users)	For 51+ Users			Discount of MRC
	Canvas Form Conversion	Quoted by Canvas			Discount of MRC
	Canvas Custom PDF Creation	Quoted by Canvas			Discount of MRC

Consutlative Hourly Rate (this rate will be included in the contract)	$0.00

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3-MCostsheet

Vendor Name:	Sprint

	Product Name	***Product Description***	***Characteristics of Product***	***Percentage Off Discount (%)****	***Notes***
	Sprint Enterprise messaging	**Sprint Enterprise Messaging Gateway (EMG):** EMG allows Customer to send messages to large numbers of Employees, including those who have Sprint devices and those who have devices from other carriers. Features include the ability to send text messages exceeding 160 characters as one message, notification of message delivery, and integration with some Customer IT systems. Except as otherwise set forth below, charges are applied at Customer's Billing Account Number (BAN) level.	Enterprise Messaging	100.00%	Public Safety Customers using Wireless Priority Service are eligible for basic 10K messages @ $60 at no cost. Additional service levels require additional charges and are not eligible for discounts.

Consutlative Hourly Rate (this rate will be included in the contract)	$0.00

.

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3-N Costsheet

Vendor Name:	Sprint

	Product Name	***Product Description***	***Characteristics of Product***	***Percentage Off Discount (%)****	***Notes***
	DataLink	Sprint Data Link provides secure, high-speed wireless connection to the corporate enterprise WAN. The product allows an end-user device to connect to the Sprint wireless network and then intelligently and securely routes user traffic back to the corporate network.	Secure LAN Access	100.00%	

Consutlative Hourly Rate (this rate will be included in the contract)	$0.00

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3-N Costsheet

Vendor Name:	Sprint

	Product Name	***Product Description***	***Characteristics of Product***	***Percentage Off Discount (%)****	***Notes***
	Columbitech	Sprint Secure Mobile VPN provides session persistence to the company VPN and protects any application on any device with the highest levels of military-grade security.	Secure LAN Access	5.00%	Discount of MRC

Consutlative Hourly Rate (this rate will be included in the contract)	$0.00

.

MA262-1 Wireless Voice, Data and Accessories Attachment C: Costsheet

Award Category 3-N Costsheet

Vendor Name:	Sprint

	Product Name	***Product Description***	***Characteristics of Product***	***Percentage Off Discount (%)****	***Notes***
	Sprint Secure WiFi	Sprint Secure Wi-Fi is an application for smartphones and tablets that automatically turns itself on and off to protect mobile users when using public Wi-Fi hotspot, such as at a	Secure LAN Access	5.00%	Discount of MRC

Consutlative Hourly Rate (this rate will be included in the contract)	$0.00

.

MA262-1 Attachment H

NASPO ValuePoint Cooperative Contract Detailed Sales Report

□ No Quarterly Sales

Contractor:

Quarter:

Vendor Name	Vendor Contract Number	State	Customer Type	Bill to Agency	Bill to City	Bill to State	Bill to Zipcode	Acct # or Customer #	Invoice Date	invoice #	Product Description	CRU Lines	CRU Minutes	CRU Text	CRU Data	monthly service cost	Equipment Lease/Rental Cost	Total cost (monthly service + lease/rental)	Admin Fee

Field Name		Field Description
VENDOR		The awarded Contractor's name
VENDOR CONTRACT NUMBER		Lead State assigned contract number (using Lead State's numbering protocol)
STATE		State postal abbreviation code (Alaska = AK, Missouri = MO, etc.)
CUSTOMER TYPE (SEGMENT)		State Gov't, Education-K12, Education-HED, Local Gov't, Medical, Other - are acceptable segments. [determined by industrial practice for each contract - uniform for each contract]
BILL TO AGENCY		Customer (agency) Bill to name
BILL TO CITY		Customer (agency) Bill to city
INVOICE DATE		(mm/dd/ccyy)
PRODUCT DESCRIPTION		Product description of purchased product
CRU Lines		Commodity-level code based on UNSPSC code rules (8 Digits)
CRU Minutes		**Number of voice minutes used**
CRU Text		**Number of texts sent and received**
CRU Data		Amount of data used
CRU Gross Sales		**Gross Sales**
Equipment Lease		**Amount of monthly charges for leased equipment**
LIST PRICE/MSRP/CATALOG PRICE		uniform for each contract]
NASPO ValuePoint PRICE		NASPO ValuePoint Price- US Currency ($99999.999)
QUANTITY		Quantity Invoiced (99999.999)
TOTAL PRICE		Extended Price (unit price multiplied by the quantity invoiced) - US Currency ($999999999.999)
NASPO ValuePoint ADMIN FEE		Administrative Fee based on Total Price - US Currency ($999999.999)

NASPO ValuePoint Cooperative Contract Detailed Sales Report

Contractor: Quarter:

Vendor Name	Vendor Contract Number	State	Customer Type	Invoice Date	IRU Lines	Total Cost	Admin Fee

Carrier lists every plan in use under the NASPO contract, provides the quantity of the lines of service using each plan and provides basic details of the plan

Line Count	Plan #	Plan Description	Discount Eligibile	Access Cost Before Discount	Included in Plan						Notes
					Voice		Data		Text	subsidized	
					Minutes	Pooled	GB	Pooled	Qty	Device	
qty devices o this plan	if carrier has one		yes / no								

MA262-1 Attachment I Award Category 2 Reporting Template

NASPO ValuePoint Cooperative Contract Detailed Sales Report

Contractor:

Quarter:

□ No Quarterly Sales

Vendor Name	Vendor Contract Number	State	Customer Type	Bill to Agency	Bill to Address	Bill to City	Bill to Zipcode	Ship to Agency	Ship to Address	Ship to City	Ship to Zipcode	Order Number	PO Date	Invoice Date	Invoice Number	Product Description	Quantity	UNSPSC Commodity	IRU or CRU	List Price/MSRP	NASPO ValuePoint Price	Total Price	Admin Fee	EPEAT	Energy Star Compliant
																								Need to match up with Green Language in RFP	

Field Name		**Field Description**
VENDOR		The awarded Contractor's name
VENDOR CONTRACT NUMBER		Lead State assigned contract number (using Lead State’s numbering protocol)
STATE		State postal abbreviation code (Alaska = AK, Missouri = MO, etc.)
CUSTOMER TYPE (SEGMENT)		State Gov't, Education-K12, Education-HED, Local Gov't, Medical, Other - are acceptable segments. [determined by industrial practice for each contract - uniform for each contract]
BILL TO NAME		Customer (agency) Bill to name
BILL TO ADDRESS		Customer (agency) Bill to address
BILL TO CITY		Customer (agency) Bill to city
BILL TO ZIPCODE		Zip code in standard 5-4 format [standard 5 digits is acceptable, formatted as a zip code]
SHIP TO NAME		Customer (agency) Ship to name
SHIP TO ADDRESS		Customer (agency) Ship to address
SHIP TO CITY		Customer (agency) Ship to city
SHIP TO ZIPCODE		Zip code in standard 5-4 format [standard 5 digits is acceptable, formatted as a zip code]
ORDER NUMBER		Vendor assigned order number
PO DATE (ORDER DATE)		(mm/dd/ccyy)
INVOICE DATE		(mm/dd/ccyy)
INVOICE NUMBER		Vendor assigned Invoice Number
PRODUCT DESCRIPTION		Product description of purchased product
UNSPSC		Commodity-level code based on UNSPSC code rules (8 Digits)
LIST PRICE/MSRP/CATALOG PRICE		List Price - US Currency ($99999.999) [determined by industrial practice for each contract - uniform for each contract]
NASPO ValuePoint PRICE		NASPO ValuePoint Price- US Currency ($99999.999)
QUANTITY		Quantity Invoiced (99999.999)
TOTAL PRICE		Extended Price (unit price multiplied by the quantity invoiced) - US Currency ($999999999.999)
NASPO ValuePoint ADMIN FEE		Administrative Fee based on Total Price - US Currency ($999999.999)
VAR/Reseller/Distributor		If a VAR/Reseller/Distributor, name of VAR/Reseller/Distributor and state where located
Energy Star Compliant		Yes = 1 No = 2 Energy Star Does not Apply = 0
Optional		More information

Provider lists each Make / Model of equipment sold and the quantity sold of each.

Quantity Sold	Equipment/ Accessory Type	Part Number	Manufacturer	Model	Discount Eligibile	List Price	Notes

yes / no

to be taken
from category
2 cost sheet
examples:
smart phone
tablet
case
etc …

MA262-1 Wireless Voice, Data and Accessories

Attachment J Award Category 3 Reporting

Vendor list Service or Product in use under the NASPO ValuePoint contract, provides the quantity of users for each and the total spend for each application

Subcategory	Vendor Contract Number	State	Customer Type	Bill to Agency	Bill to City	Bill to State	Bill to Zipcode	Acct # or Customer #	Invoice Date	invoice #	Service / Application Name	Quantity of Systems	Quantity of Users or endpoints	# users in largest system	Total Spend
3A, 3 B, 3C, etc…															

The following section requests a description of the characteristics of the networks that you will be using to provide the services covered by award Category 1 of this RFP. To understand the infrastructure and context in which your services will be offered, we ask that you please describe your existing networks, technologies, and plans.

1. 4G Cellular Services

Describe the current status and plans for your 4G LTE and earlier generation wireless voice/data technologies.

Sprint 4G LTE offers next-generation wireless data service, with turbocharged speeds many times that of 3G. Offering significantly lower latencies than 3G, Sprint 4G LTE permits migration from fixed to mobile for many delay-sensitive applications, such as video streaming, video teleconferencing and interactive business applications that you can rely on to deliver critical information in real time.

Sprint 4G LTE also provides the network capacity to support the exploding demand for high-speed connectivity from a new generation of devices and applications. Sprint's continuing deployment of advanced 4G LTE techniques such as carrier aggregation and beamforming (LTE Plus) are dramatically improving utilization of our enormous 2.5 GHz spectrum assets, giving Sprint a significant advantage over our competitors as capacity requirements continue to increase.

What is Sprint 4G LTE?

Sprint 4G LTE offers you the following advancements to improve your mobile experience:

- **More Bandwidth:** You can run bandwidth-hungry, latency sensitive applications – video conferencing, batch data runs, cloud migrations, etc. Sprint 4G LTE gives you the capacity you need to mobilize your workforce and maintain business continuity.
- **Higher Data Speeds:** Almost anywhere with 4G LTE, you will experience data speeds ten times faster than 3G, with average downloads of 6-8 Mbps and uploads of 2-3 Mbps, which enables video and other data intensive applications. In locations with LTE Plus, average speeds are many multiples of this.
- **Reliable Coverage:** Powered by our cutting–edge network, 4G LTE customers now also experience better in-building coverage and more reliable coverage overall. The higher the frequency, the harder it is for radio signals to penetrate walls and travel distances. But our 800MHz spectrum coupled with HPUE devices mean Sprint can deliver improved, consistent in-building performance and reach locations not previously accessible.
- **Lower Latencies:** Latencies of less than 60 milliseconds, nearly half that of 3G, for delay-sensitive applications. In areas with LTE Plus, latencies are even lower.

Where is 4G LTE?

Sprint is focused on leveraging its spectrum portfolio to provide a network that delivers the consistent reliability, capacity and speed that you demand. Having completed our 4G LTE rollout across our traditional Sprint 1.9 GHz network, Sprint continues to augment coverage, capacity, and speed with our 800 Mhz and 2.5 GHz spectrum. As a result, network performance and coverage continues to improve:

- 4G LTE service now in 868 U.S. markets covering over 304 million people
- 2.5 GHz deployment now covering 125 million people, improving speed and capacity
- Nationwide 800 MHz deployment, offering improved in-building and other coverage
- Recent third-party awards for reliability and performance in cities across the country

With Sprint 4G LTE businesses, consumers and government customers can extend their full internet experience with excellent speeds and the widest array of devices. These speeds, combined with much lower latencies enable many higher-bandwidth and latency-sensitive applications that are poorly served by 3G networks:

Sprint LTE Plus

As a result of our Network Vision network overhaul, Sprint offers not only 4G LTE, but a whole new era in wireless communications: Sprint LTE Plus. Sprint LTE Plus is a powerful network capability that utilizes up to three bands of LTE to create a revolutionary network experience. Given Sprint's deep spectrum and technology assets, Sprint LTE Plus promises the technical feasibility to deliver up to 2 Gbps peak speeds. After several years of network upgrades, we are positioned to take advantage of the latest technologies to offer you the coverage, reliability, and data speeds on which your people depend.

Sprint LTE Plus comes to life for customers via their devices. With the 4G LTE improvements in speed and latency, your staff will enjoy:

- **Connectivity**: Improved access to the internet and corporate networks, improving performance of data-intensive and delay-sensitive applications to provide a competitive advantage.
- **Speed**: New applications on smartphones, laptops, tablets and similar devices with higher speeds and higher capacity than 3G.
- **Mobility**: Convenient access for employees who cannot afford to wait for a connection.
- **Security**: Built-in, robust security designed to protect sensitive data.
- **Choice**: No need to switch wireless voice providers. Sprint 4G LTE is offered as a separate data service.

Building on Network Vision's multimode capability, Sprint LTE Plus is designed to accommodate all of Sprint's spectrum bands on a single device. These devices use the spectrum dynamically, transparently shifting from one band to another depending upon factors like location or the type of application being used, offering you the best possible customer experience:

- 50-60 Mbps peak speeds and 6-15 Mbps average speeds today, with potential for increased speeds over time
- For business customers, this means unprecedented data speeds, stronger in-building signal and improved call quality & clarity

Sprint's continuing deployment of advanced 4G LTE techniques such as carrier aggregation and beamforming (LTE Plus) are dramatically improving utilization of our enormous 2.5 GHz spectrum assets, giving Sprint a significant advantage over our competitors as capacity requirements continue to increase:

- **Carrier Aggregation/LTE Advanced (LTE Plus)**: with the unique characteristics of Sprint's abundant 2.5 GHz spectrum, Carrier Aggregation and other LTE-Advanced technologies offer supercharged data speeds with future potential for speeds in the gigabytes. Compared to current 4G LTE networks, these techniques offer capabilities such as:
    - Average download speeds of 12-30 Mbps in LTE Plus areas
    - Buffer HD video in 10 seconds vs. 1 minute
    - Download 60 min. HD show in 2.5 minutes vs. 35 minutes
    - Download 60 min. podcast in 7 seconds vs. 52 seconds

- **Beamforming**: Sprint 4G LTE is taking advantage of a spatial multiplexing technique known as beamforming, where data streams are focused on only the strongest layers, thus focusing power in the most efficient way. With multi-layer beamforming, different data can be transmitted on different layers, increasing spectral efficiency by improving the signal-to-noise-plus-interference ratio (SNIR) and thus further improving capacity.

1. Current 4G network coverage across the U.S.

Sprint's 4G LTE network coverage is in 260 markets, covering over 286 million people, and the ultra-high speeds of LTE Plus in 250 markets. Including roaming and partner networks, Sprint's wireless voice and data coverage is currently available to over 322 million people in the United States, including Puerto Rico and the U.S. Virgin Islands.

Our LTE Plus is currently covering 237 major markets with 2 channel Carrier Aggregation, offering peak speeds of 50-60 Mbps and 3-channel capable of up to 300 Mbps! We plan to increase both those maximums and the availability of LTE-Advanced technologies in the coming years as deployment of these techniques matures.

2. Major planned enhancements for these and earlier generation networks in light of the deployment of 5G-based services

We are leveraging our large and diverse spectrum assets to offer:

- **Nationwide 4G LTE Network**: Using all of Sprint's spectrum assets, depending on location, our 4G LTE network offers coverage to over 304 million people nationwide with:
  - Typical download speeds of 6-8 Mbps or better
  - Upload speeds in the range of 2-3 Mbps
  - Network latencies averaging less than 60 milliseconds
- **Upgraded 3G Network**: Taking advantage of our 800 MHz spectrum to improve our 3G coverage and reliability:
  - Fewer dropped calls
  - Stronger indoor signals
  - Expanded coverage area
  - Faster downloads
- **Upgraded Backhaul:** Sprint is upgrading its backhaul network to a more efficient, scalable Ethernet connection that will allow for continued expansion as data requirements continue to explode. Upgraded backhaul means:
  - More efficient data delivery to your mobile devices and tablets
  - Increased support for new 4G LTE network technology
  - An estimated 20x more bandwidth capacity so you don't lose connection in high-traffic areas
- **HD Voice**: Now available nationwide and on most Sprint devices, HD Voice creates a whole new era in the wireless voice experience:
  - Virtually eliminating most background noise and dramatically enhancing sound quality, HD Voice is revolutionizing expectations for wireless voice calls.
  - Both callers must have HD-capable devices, and both must be on Sprint's upgraded network. Roaming partners and some affiliate areas may not have this upgrade.

3. Voice Quality Performance Target/Guarantee

a. Mean Opinion Score (MOS) rating for voice calls

b. Dropped Call Percentage

c. What improvements do you expect with the introduction of VoLTE and Wideband Voice?

In response to the above, Sprint constantly monitors our wireless network to provide the best call quality possible and MOS is one of the measures used. However, since the network is in a constant state of flux and there are so many variables affecting perceived call quality, e.g. location of caller, stationary or moving, device type, headset or no headset, Bluetooth or no Bluetooth, etc., MOS scores will vary significantly. For this reason, Sprint does not publish MOS information. Wireless voice networks generally tends to score in the range of 3 – 3.5 depending on the variables above and other factors.

A frequent call quality issue with wireless communications is background noise. Sprint has addressed this issue with High-Definition (HD) Voice, a Sprint standard for mobile phones where background noise is virtually eliminated and sound quality is dramatically enhanced. HD Voice is designed to provide a better experience than a landline. A typical phone without HD Voice offers four octaves of sound, but a phone with HD Voice offers seven (10 octaves is considered perfect hearing).*
** Available only when both callers are using HD Voice capable devices.*

Sprint has enhanced our Wi-Fi Calling platform to offer the capability to use the Sprint LTE network for voice calls on select devices with Calling Plus. Calling PLUS allows VoIP call origination on the Sprint LTE network and seamless call continuity between Wi-Fi and LTE ahead of our VoLTE commercial deployment, which will provide simultaneous voice and data once it is fully launched. You can now talk, text and surf simultaneously. Get more done in less time!

4. Broadband Data Performance Expectations/Guarantees:

d. Uplink/Downlink Data Rates (Peak, Sustained, Cell Edge)

Anywhere on the Sprint 4G LTE Network, users will experience:

- Average download speeds of 6-8 Mbps
- Average upload speeds of 2-3 Mbps
- Peak speeds of 25 Mbps
- Average device to network edge round-trip latency of less than 60ms

Extended/Roaming speeds:

- Extended 4G LTE / LTE Roaming speed average download 1-6 Mbps, average upload 1-3 Mbps
- Extended Non-LTE Roaming speed avg. download 50 Kbps - 700 Kbps, avg. upload 50 Kbps - 70 Kbps
- Roaming: Average download 50 Kbps - 64 Kbps, Average upload 50 Kbps - 70 Kbps

In select areas, users with 2x Carrier Aggregation compatible devices will experience:

- Average download speeds of 12-30 Mbps
- Average upload speeds of 2-3 Mbps
- Peak speeds of 100+ Mbps[1]

Users with 3x Carrier Aggregation compatible devices will experience peak download speeds greater than 200 Mbps.

e. Latency

Latency is affected by the over-the-air radio spectrum used by commercial wireless carriers and the backhaul to cell sites. With improved technologies for data users and devices now utilizing faster processors, improved memory capacity and more efficient operating systems, overall latencies on Sprint's wireless networks are coming down.

Average latencies experienced by Sprint customers depend on the network technology in a given location:

- 4G LTE average latencies are: less than 60 milliseconds
- 3G (EVDO rev A) average latencies are: 160 milliseconds

When roaming on 1xRTT networks, typical end-to-end latencies are 400-800 milliseconds.

These numbers are actually averages with the low end reflecting the average latency for a 1 hour interval with approximately 1 megabyte of content-driven traffic. The high end reflects the same period of time assuming a startup from a "dormant" condition. The theoretical minimum for 1xRTT is approximately 200 milliseconds.

5. Mobile E911 Technology

f. Technology employed?

Technology employed is CDMA, device-based, A-GPS, with network-based AFLT fallback.

g. Location Accuracy?

Small cells are considered part of the macro network infrastructure for purposes of location accuracy. VoWi-Fi utilizes a combination of reliance on the wireless macro network signal, where available, with fallback to routing over Wi-Fi to a VoIP solution.

Sprint is investing and developing integration technologies for the National Emergency Address Database so that Dispatchable Location can be provided when WiFi access points are detected by a wireless device. Sprint is also working closely with wireless device vendors to leverage new device-based hybrid location technologies to improve indoor location performance. Part of Sprint's device portfolio already leverages device-based hybrid technology for emergency services.

h. Indoor versus outdoor accuracy?

No distinction currently for indoor versus outdoor accuracy.

i. Compliance with February 2015 FCC Mandates

Sprint is compliant with FCC 4th Report & Order "Wireless E911 Location Accuracy Requirements" (PS Docket #07-114) released on February 3, 2015. Within the order there are major components to the timelines and provisions adopted in the order for national carriers:

1. Horizontal Location which requires CMRS providers to provide (1) Dispatchable location , or (2) x/y location within 50 meters and a 6 year scale starting @ 40% in year 2 (2017) going to 80% by year 6 (2021).
2. Vertical Location which required the making uncompensated barometric data available to PSAPs from handsets capable of delivering barometric sensor data and use of an independent test bed process to develop a proposed z-axis accuracy metric within 6 years.
3. Reporting and Compliance Measures in which the order adopted six monitoring cities by which ongoing reporting is required.

j. Technology Plans/Expectations/Timeframes

Sprint participates in the industry related work groups developing the required National Emergency Address Database (NEAD) and those work groups and committees developing standards for the new technologies and the various components of the order. Sprint continues to improve our network overall for voices & data services.

2. Network Reliability, Disaster Recovery and Business Continuity

Describe your overall disaster preparedness plan, the steps you have taken to safeguard your internal and exposed assets, and the types of services and response we can anticipate in the event of an emergency or a disaster.

Sprint's Business Continuity Management Team works as a customer advocate when large network outages occur. The team works closely with network recovery teams to establish customer prioritization once the backbone, TSP (Telecommunications Service Priority) and Critical Life Circuits are re-established. Sprint has an established cell site classification and service restoration process.

Sprint’s preparedness with hardware/systems at an alternate site is as follows:

If referring to a Sprint Data Center, the IT Incident Management Team identifies and prioritizes the recovery of IT applications process following the business strategy of “Serve, Sell, Bill, Report”. This criterion allows IT to assess and align each application based on the business function and impact to Sprint. An application alignment process is used to determine the priority of the application in the recovery timeline.

If referring to Network Assets, Sprint's Network Team compliments its assets with third parties when large network outages occur. Sprint has a very robust emergency response and disaster recovery plan which enables quick restoration of impacted services following a disaster. Sprint mitigates congestion risks through traffic management algorithms to handle the overload surges in traffic. Additionally, Sprint’s well trained and exercised disaster recovery response teams proactively monitor congestion and performance of the wireless network and determine the appropriate course of action. This may include performing parameter changes, adding additional capacity to the network via radio installations to cell sites and/or by adding additional backhaul. Cell Site On-Wheels (COW) and Satellite On-Light-Trucks (SatCOLT) may also be used to replace and/or expand Sprint’s foot print or add additional capacity to the network. Engineers use traffic history to provision network resources to support busy-hour traffic for cellular networks. Third parties are used to perform various functions such as reconnaissance, generator deployment/refueling, equipment repair, etc.

1. **Describe your overall approach to network hardening, including physical security for exposed assets, redundant links to cell sites, and internet-initiated threats.**

National Security & Compliance (NSC)

The NS&C team works to improve the physical and cybersecurity of Sprint’s critical infrastructure and facilitates information sharing within and across the communication industry and government. Today’s threat environment highlights the need to protect our Nation’s critical functions that support national and economic security and public safety. A partnership leveraging public and private sector capabilities is essential for providing a realistic approach for protection and response.

The NS&C team is the primary point of contact to the Department of Homeland Security during times of increased threat or attack and during significant all hazards events. Members of the NS&C team serve as Sprint’s onsite representatives at the Department of Homeland Security’s National Coordinating Center (NCC) for Communications; to provide a line of communication between corporate leadership, other telecommunication providers and government officials. This partnership supports the mission of the NCC who leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework.

- Sprint's Information Security Policy and Information Handling Requirements require that any restricted data being transmitted anywhere external to the Sprint network must be encrypted in transit and storage using a strong industry standard algorithm. We deploy a layered security architecture for the protection of all networks, systems and data. Sprint networks are also protected by a logical DMZ to prevent unauthorized tampering. In addition, our Cyber Incident Response Plan addresses insider threats as well as external threats and is tested periodically.

- Sprint IP networks are designed with security balance to provide confidentiality, integrity, and availability. The primary focus is on availability to our customers as a network transport provider, which results in a majority of the security overhead being applied at the customer end-points.

Network Incident Management Team

Network Services' implementation of the Incident Command System (ICS), stays true to the principles of ICS. This enables Sprint to leverage this best practice in wide-scale responses, using common terminology and standard organizational structures to communicate efficiently internally and with external customers such as Public Safety agencies as many of these agencies utilize ICS. Teams train on and deploy in standard ICS sections, branches, units and strike teams, and emphasize span of control, comprehensive resource management, and other ICS principles.

Network teams leverage Sprint tools such as hardened GPS-enabled phones, wireless modems, custom applications, M2M solutions and smart phones to aid in situation assessment, response and resource tracking. The teams also maintain a pool of Satellite phones as a contingency for use in restoration. Teams continue to create innovative response tools, such as the unique backhaul called Satellite Cell on Light Trucks (SatCOLTs) that enable restoration of service when a traditional backhaul is not available.

When the Network IMT receives notification of an actual or potential situation that requires activation (hurricane, earthquake, regional power outage, other event where business as usual would not resolve the situation), a virtual Emergency Operations Center (EOC) is established. This EOC performs an initial overall assessment, establishes monitoring bridge(s), coordinates between agencies impacted by the event, assigns tasks, gathers status information and performs executive notifications at prescribed times.

Cell Site Disaster Planning

Sprint's priority site restoration plan focuses resources and expedites recovery by making sure that existing infrastructure is operating properly under normal circumstances and by having a response plan for abnormal circumstances. To accomplish this, Sprint has implemented a detailed preventative maintenance program to insure all systems and redundant equipment are in proper working order. Sprint sites are equipped with battery backup. Some sites have fixed generators or fuel cells for additional back-up power. Sprint maintains a fleet of mobile generators deployable to Sprint service areas. Formal cell site classification designates all sites for criticality. Prioritization aids in properly allocating response personnel, generators and other resources.

Cellular Network Disaster Planning

Communications from Sprint cell sites are backhauled with various combinations of Ethernet, copper, fiber, and microwave systems. Most Sprint hub locations are placed on bi-directional fiber rings. These rings significantly reduce the chance of network failure due to third party fiber damage, equipment failures or other potential causes of service interruptions. Sprint's radio network provides significant overlapping coverage areas which often allow cell sites to fully or partially compensate for a neighboring cell site. In an effort to minimize service impact when a site is down, Sprint maintains a fleet of Cell Sites on Wheels (COWs) which are portable self-contained cell sites. COWs can be deployed to restore coverage from a damaged site or provide additional capacity in the immediate vicinity of an incident.

Switch Disaster Planning

Sprint has implemented a distributed architecture for interconnection redundancy utilizing dual fiber facilities at switch locations. Switch locations have battery backup as well as permanent generators. In addition, site recovery plans have been developed for all major switch locations, prioritizing available options for relocation, and ensuring agility when faced with disaster recovery issues. Most switches also have tap boxes that readily connect to the output of a portable generator in the event of primary generator issues.

Overall Network Performance Management Efforts

The performance of Sprint's networks is monitored 24 hours a day, 7 days per week and 365 days a year by the Network Monitoring Centers. In addition, local switching offices staffed by trained technicians and management coordinate with these larger operations centers, to ensure that Sprint's networks are properly maintained.

Network Restoration Prioritization

Sprint's Business Continuity Management Team works as a customer advocate when large network outages occur. The team works closely with network recovery teams to establish customer prioritization once the backbone, TSP (Telecommunications Service Priority) and Critical Life Circuits are re-established. Sprint has an established cell site classification and service restoration process.

Special Event Planning

Special events have the potential for adversely affecting the customer experience due to greatly increased wireless traffic demands. Sprint has a mature special events process with dedicated project management personnel and a cross-functional management tool. Teams archive records of recurring special events and leverage capacity planning teams in implementing enhancements to optimize the customer experience. Sprint has used its experience in managing very large temporary users at NASCAR events to manage other special events. As an example, Sprint interfaces with the NCC (National Coordinating Center for Communications) in managing capacity needs at National Special Security Events, NSSE.

2. What are your greatest challenges in terms of recovery in the event of extensive damage throughout an extended area, and how do you address them.

As businesses, government agencies, and individual consumers become more and more reliant on wireline and wireless communications, as well as remote access to information, the concept of business continuity has never been more important. Sprint incorporates business continuity as part of the corporation's overall business philosophy. This philosophy promotes utilizing business continuity principles, guidelines, and standards by all company employees during routine business operations to assure the continuation of Sprint's mission critical business operations and services. The goal of Sprint's Business Continuity (BC) program is to minimize financial damage and damage to Sprint's brand, its employees and customers, following significant business disruptions.

Industry accepted principles are the basis for Sprint's BC program. Sprint has adopted key principles from standards set by organizations such as the Disaster Recovery Institute International (DRII), ASIS Organizational Resilience Standard, Federal Emergency Management Agency (FEMA), Business Continuity Institute (BCI), American National Standards Institute (ANSI), NFPA 1600, International Organization for Standardization (ISO) 27001 and ISO 22301 and several Military Specifications (Mil-Spec) standards. Sprint's Business Continuity Program Overview is reviewed and approved on an annual basis.

Sprint Business Continuity Mission Statement

To assure the continuation of Sprint's mission critical business operations and services, minimize risks to Sprint's employees and customers, as well as damage to Sprint's brand and services, following significant business disruptions.

Executive Sponsorship and Program Governance

A comprehensive business continuity program requires executive sponsorship, a structure for decision-making, and a means to direct and manage incremental changes towards goals and objectives. Sprint's program governance structure achieves each of these requirements and accomplishes them through inclusion and diversity of thought and viewpoint. Sprint Business Continuity Program Governing Principles:

- Committed to employee and customer safety
- Committed to preserving business operations and service to Sprint customers
- Business continuity is a shared responsibility across all levels of management, all business units (BUs), the Business Continuity (BC) professionals within the BUs and the Business Continuity Office (BCO)
- Business continuity professionals and Incident Management Teams (IMTs) must be knowledgeable, well trained and prepared to respond when activated
- Continual improvement, flexibility and maturity is necessary for success

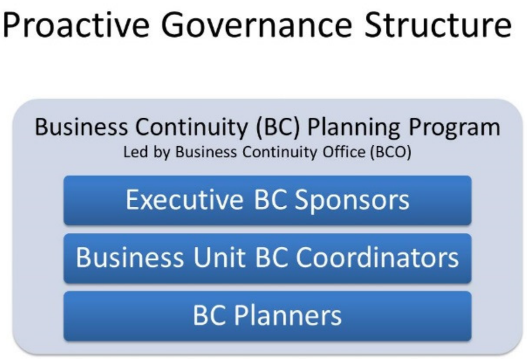
The following describes the program governance structure that begins with the highest levels of the company and leverages management and expertise for optimal effectiveness.

- **Executive Business Continuity Sponsors**: BU senior level executive sponsors promote business continuity awareness, performance and maturity among all areas of the company. Each sponsor assigns subject matter experts and BC coordinators to make available appropriate resources to BC planning efforts for their business unit. The executive sponsors provide support to Sprint's Business Continuity Office (BCO) in overseeing BC-related activities, performance and ensuring adherence and accountability of Sprint's BUs to BC program policies and standards.

- **Business Continuity Office (BCO)**: The BCO is responsible for establishing the policy, structure, and methodology for developing, maintaining, and testing enterprise-wide BC and Disaster Recovery (DR) plans. During an incident, the BCO is responsible for coordinating cross-functional incident management activities of Sprint's Enterprise Incident Management Team (EIMT) and informing senior leadership of impacts and progress.

- **Business Unit Business Continuity Coordinators**: BC coordinators are accountable for BU planning implementation and completion in accordance with BC program elements, as defined by the BCO, for their assigned department and executive sponsor.

- **Business Continuity Planners**: BC planners are responsible for documenting and maintaining business continuity plans in Sprint's Business Continuity Management System (BCMS).


Proactive Governance Structure
Business Continuity (BC) Planning Program
Led by Business Continuity Office (BCO)
Executive BC Sponsors
Business Unit BC Coordinators
BC Planners

Risk Management

Upon identification of potentially significant risks, Sprint makes every attempt to mitigate and plan for any eventuality that could affect Sprint's customers and employees. Sprint's business continuity risk program is integrated with the company's Enterprise Risk Management (ERM) process led by Corporate Audit Services (CAS) which plays a critical role in Sprint's overall success by partnering with business units to manage risk and optimize business performance. CAS has the unique opportunity to touch all facets of the company and interact with all levels of management in providing unbiased, risk-based assessments of business processes.

Risk Council: The ERM includes a Risk Council on which Managers and Directors sit. The Risk Council's purpose is:

- Risk identification
- Risk self-assessment
- Strategy and actions to address risk within policy
- Ensure compliance with ERM policies and procedures
- Provide assertions on risk exposure

Risk Steering Committee: The Risk Steering Committee is made up of Vice Presidents and Senior Vice Presidents. Their purpose is:

- Provide a strategic view of risk
- Recommendation of key risks/unforeseen events

Business Impact Analysis

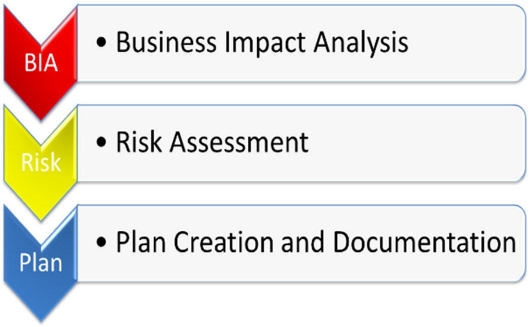
Through various forms of examination, including Business Impact Analysis (BIA), criticality of every part of the business (business processes, applications, suppliers, partners, sites, network elements and other business aspects) is determined. The criticality defines how long these elements can be disrupted without significant impacts to the company's employees, customers, operations and/or assets. This prioritization drives mitigation and planning decisions. Critical business processes require a comparable criticality assigned to the applications they use, the suppliers they need and other dependencies. Sprint's classification levels for criticality include, but are not limited to, Mission Critical, Business Critical, Enhanced Support and Standard Support.

BIA reviews are conducted on a scheduled basis according to the criticality of the process, system or application. The processes, systems and applications deemed most critical are reviewed on a more frequent basis than those that are less time sensitive.

Business Continuity Strategies and Planning

Sprint uses an internally developed maturity model for benchmarking the BC program success and progress. The model is based on the Capability Maturity Model as developed by Carnegie Mellon University.

Business Continuity Planning Process



- Process, Standards & Documentation – Common terminology, methodologies and formal documentation on standards and procedures help our large company stay consistent and current. All key stakeholders are responsible for reviewing program documents at least annually.
- Reporting – Each year, the Business Continuity Office formally reports to Sprint's Executive Management on the efforts and status of the Business Continuity Program and partners with Corporate Audit on reporting risk information to the Board of Directors.
- Maintenance – Frequent reviews of plan details and processes are updated in a timely manner, following changes to contacts, suppliers, processes, organizational structures, etc.
- Supplier Business Continuity – Evaluation process of business continuity plans for key partners, suppliers and vendors of which Sprint is dependent upon.

Analysis of potential vulnerabilities and/or new emergent threats is completed on a regular basis. The BCO is responsible for development and implementation of enterprise strategies available to all BC Planners for use in the BC planning and maintenance processes. Examples of enterprise strategies include:

Alternate Site and Remote Access

Sprint utilizes information obtained through BIA and risk reduction strategies in order to preserve business functions that are required in the face of a disaster. Depending on the size and scale of the event, Sprint has strategies in place to provide added capacity, alternative work locations and remote access if necessary to retain operations.

Business functions that require alternate sites, geographic redundancy and remote access capabilities are identified proactively and plans are periodically reviewed and revised as necessary in anticipation of any event. As Sprint has international operations, alternate site locations vary.

Employee Continuity

Sprint has matured its former “Pandemic Continuity” Plan into “employee continuity” plans which incorporate events that may result in employee injuries or fatalities or significant and sustained employee absenteeism. Examples include a pandemic or infectious disease that poses life-threatening risks to employees and their families, a company-owned building roof collapse, or an unplanned school closing due to a natural or a man-made disaster requiring parents to be absent from the work place. Sprint has a designated internal structure responsible for impact assessments and decision making during an employee continuity event as well as proactive planning to identify emerging threats and new strategy implementation. As Sprint’s business continuity plans are developed with an “all-hazards” mindset, employee continuity strategies such as remote work, increased office cleanings and social distancing are considered in all plans.

Continuous Improvement and Maturity

In BC planning, as in other disciplines, it is important to document and test plans for effectiveness. Based on the results, updates to the plans are made. That is the basis of the **Plan-Do-Check-Act** model.

In the **Plan** phase, teams and experts analyze conditions and capabilities and devise objectives, controls, processes and systems to improve Sprint’s ability to prepare or respond to a disruption.

In the **Do** phase, teams exercise or implement the elements according to the plan(s) and ensure they operate according to assumptions/beliefs. This phase may include a test, exercise or real disruption requiring business continuity plan execution.

Exercises

Sprint’s response organizations use exercises to evaluate plans, educate personnel, test functions, and operational capability. Sprint conducts at minimum an annual exercise of its business continuity plan. Additionally, as part of the nation’s critical infrastructure, Sprint participates in coordinated situation drills with FEMA, the Department of Homeland Security (DHS), and state emergency management agencies to ensure coordinated preparedness and response during a disaster. The most common types of exercises conducted are tabletop, walk-through, and functional drills. The type of exercise varies as they are dependent upon needs assessments, priority, recent plan executions, budget, etc. Information related to these exercises is proprietary to Sprint.

In the **Check** phase, teams monitor and review the performance of the plans and look for opportunities for improvement. In many cases, lessons are learned from actual practices that were missed in the Plan phase. Lessons learned may be obtained from tests, exercises or real disruptions requiring business continuity plan execution.

After Action Reviews (AAR)

Following an exercise or a plan execution in response to a disruption, an AAR is conducted to ask participants to identify areas of success and improvement. These are documented as lessons learned and tracked to satisfactory completion in the **Act** phase.

In the **Act** phase, changes may be necessary to the original objectives, controls, processes and systems in the original plan(s). It may be necessary to upgrade capabilities in a specific area or to change tactics or strategic assumptions. Plan(s) are then updated in accordance with lessons learned in the Do, Check and Act phases. Once plans are updated, the cycle resumes, resulting in continuous improvement.

Awareness and Training

Sprint's Business Continuity Office (BCO) is responsible for assessing business continuity awareness and training needs of the company's employees and management so that they are prepared to respond during an incident.

Awareness

On an annual basis the BCO leads a cross-departmental awareness committee whose charter is to identify appropriate opportunities to promote BC awareness and to plan and conduct campaigns and events to meet the needs of employees. The committee develops an annual BC awareness calendar at the beginning of each year with the intent to target specific, recurring events with a messaging campaign. The awareness program covers all aspects of the BC discipline and targets different audiences with specific messaging and information that is appropriate for their role in the company.

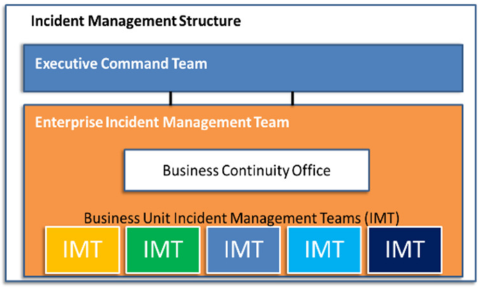
Training

Sprint's business continuity training program covers all aspects of the BC discipline and targets different audiences with specific messaging and information that is appropriate for their role in the company. Training also covers tools such as the Business Continuity Management System (BCMS) and the use of Sprint's mass notification system, for employees who have roles in incident response. Members of Sprint's Enterprise Incident Management Team (EIMT) are required to participate, at minimum annually, in enterprise training sessions facilitated by the BCO.

Additionally, an annual, all-employee policy compliance certification program includes elements of business continuity awareness and training.

Incident Management and Crisis Communications

Knowing that unexpected events occur, Sprint's Incident Management and Crisis Communications teams are highly trained and tested. As with the overall program governance structure, full executive support and authority is integrated into the incident management structure. Sprint's seasoned professionals, across multiple fields of expertise, have responded to a wide variety of major disasters.

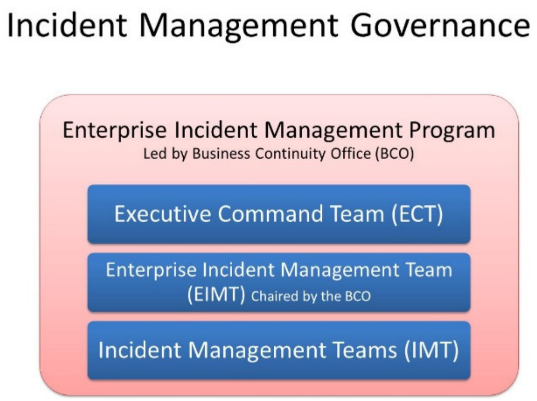

Incident Management Structure
Executive Command Team
Enterprise Incident Management Team
Business Continuity Office
Business Unit Incident Management Teams (IMT)
IMT
IMT
IMT
IMT
IMT

Executive Command Team (ECT) – The Executive Command Team (ECT) is a select group of the senior leadership team with the highest level of authority for strategic and/or tactical decisions in response to an incident. The Chief Executive Officer (CEO) is the Chairperson of the ECT. During a disaster, the ECT is kept apprised of all activities and status. If the incident requires senior executive involvement, the ECT members engage to provide guidance and approval to make necessary response and recovery decisions.

Enterprise Incident Management Team (EIMT) – Chaired by the Business Continuity Office (BCO), the Enterprise Incident Management Team (EIMT) convenes quickly as a way of sharing impact, status and critical decision-making during an incident. This team is flexible and scalable and considers many different threats and hazards as well as the likelihood they will occur.

Incident Management Teams (IMTs) – An IMT consists of members of a single business unit and is designed to meet the needs of the company, customers and employees at the time of an incident. IMTs are of varying size and complexity, capable of responding quickly and effectively to a wide array of issues. Each IMT has a designated chairperson that represents their organization on the EIMT call when the incident requires an EIMT response posture.

Crisis Communications Team (CCT): During an incident, communication needs are more urgent and requiring tailoring depending on the information and the audience. Corporate Communications, Human Resources (HR) and Legal IMTs form Sprint's Crisis Communications Team (CCT). The CCT is responsible for complex and targeted internal communications to employees and/or management and for media and public relations.


Incident Management Governance
Enterprise Incident Management Program
Led by Business Continuity Office (BCO)
Executive Command Team (ECT)
Enterprise Incident Management Team (EIMT) Chaired by the BCO
Incident Management Teams (IMT)

Information Technology

IT Continuity, Planning and Recovery (CPR) proactively integrates business continuity and disaster recovery methodology into every phase of IT Operations in order to facilitate rapid response and resolution to any critical business disruption. The IT CPR process is developed to minimize the incident duration and expedite and control the recovery efforts. IT CPR provides a structured approach for responding to unplanned incidents that threaten IT infrastructure, which includes hardware, software, networks, processes and people. IT CPR is responsible for business continuity planning for all IT assets located in Data Centers, Sprint owned Call Centers, Retail Stores and general office facilities.

Application Recovery Strategy: IT identifies and prioritizes the recovery of IT applications process following the business strategy of "Serve, Sell, Bill, Report". This criterion allows IT to assess and align each application based on the business function and impact to Sprint. An application alignment process is used to determine the priority of the application in the recovery timeline. These priorities relate to the tolerance level of the applications and systems and the length of downtime after a disaster. Recovery time objective(s) (RTO) and recovery point objective(s) (RPO) are assigned.

Data Center Resiliency Planning: Sprint Data Centers are held to exceptionally high and stringent industry standards, but more importantly, self-imposed standards of structural design, engineering, technology, redundancy, security, maintenance and 24x7 operations. Data Centers are geographically diverse and serve as alternate site failovers for each other. Strategic IT vendors critical to Sprint operations are in scope for IT Continuity, Planning and Recovery (CPR) planning solutions.

Sprint Contact Center IT Resiliency Planning: Sprint contact centers have proven failover processes. IT CPR is responsible for providing the centers with recovery planning for IT assets such as:

- Network
- Desktop
- Server
- Voice Technologies

Sprint Retail Store IT Resiliency Planning: IT CPR provides support to Retail facilities by leveraging existing Sprint strategies to ensure functionality and communications between stores and the Sprint Enterprise.

National Security & Compliance (NSC)

The NS&C team works to improve the physical and cybersecurity of Sprint's critical infrastructure and facilitates information sharing within and across the communication industry and government. Today's threat environment highlights the need to protect our Nation's critical functions that support national and economic security and public safety. A partnership leveraging public and private sector capabilities is essential for providing a realistic approach for protection and response.

The NS&C team is the primary point of contact to the Department of Homeland Security during times of increased threat or attack and during significant all hazards events. Members of the NS&C team serve as Sprint's onsite representatives at the Department of Homeland Security's National Coordinating Center (NCC) for Communications; to provide a line of communication between corporate leadership, other telecommunication providers and government officials. This partnership supports the mission of the NCC who leads emergency communications response and recovery efforts under Emergency Support Function #2 of the National Response Framework.

Network

As a Mobile Telecommunications Leader, the resiliency of Sprint's network is of paramount interest to our customers.

Network Incident Management Team

Network Services' implementation of the Incident Command System (ICS), stays true to the principles of ICS. This enables Sprint to leverage this best practice in wide-scale responses, using common terminology and standard organizational structures to communicate efficiently internally and with external customers such as Public Safety agencies as many of these agencies utilize ICS. Teams train on and deploy in standard ICS sections, branches, units and strike teams, and emphasize span of control, comprehensive resource management, and other ICS principles.

Network teams leverage Sprint tools such as hardened GPS-enabled phones, wireless modems, custom applications, M2M solutions and smart phones to aid in situation assessment, response and resource tracking. The teams also maintain a pool of Satellite phones as a contingency for use in restoration. Teams continue to create innovative response tools, such as the unique backhaul called Satellite Cell on Light Trucks (SatCOLTs) that enable restoration of service when a traditional backhaul is not available.

When the Network IMT receives notification of an actual or potential situation that requires activation (hurricane, earthquake, regional power outage, other event where business as usual would not resolve the situation), a virtual Emergency Operations Center (EOC) is established. This EOC performs an initial overall assessment, establishes monitoring bridge(s), coordinates between agencies impacted by the event, assigns tasks, gathers status information and performs executive notifications at prescribed times.

Cell Site Disaster Planning

Sprint's priority site restoration plan focuses resources and expedites recovery by making sure that existing infrastructure is operating properly under normal circumstances and by having a response plan for abnormal circumstances. To accomplish this, Sprint has implemented a detailed preventative maintenance program to insure all systems and redundant equipment are in proper working order. Sprint sites are equipped with battery backup. Some sites have fixed generators or fuel cells for additional back-up power. Sprint maintains a fleet of mobile generators deployable to Sprint service areas. Formal cell site classification designates all sites for criticality. Prioritization aids in properly allocating response personnel, generators and other resources.

Cellular Network Disaster Planning

Communications from Sprint cell sites are backhauled with various combinations of Ethernet, copper, fiber, and microwave systems. Most Sprint hub locations are placed on bi-directional fiber rings. These rings significantly reduce the chance of network failure due to third party fiber damage, equipment failures or other potential causes of service interruptions. Sprint's radio network provides significant overlapping coverage areas which often allow cell sites to fully or partially compensate for a neighboring cell site. In an effort to minimize service impact when a site is down, Sprint maintains a fleet of Cell Sites on Wheels (COWs) which are portable self-contained cell sites. COWs can be deployed to restore coverage from a damaged site or provide additional capacity in the immediate vicinity of an incident.

Switch Disaster Planning

Sprint has implemented a distributed architecture for interconnection redundancy utilizing dual fiber facilities at switch locations. Switch locations have battery backup as well as permanent generators. In addition, site recovery plans have been developed for all major switch locations, prioritizing available options for relocation, and ensuring agility when faced with disaster recovery issues. Most switches also have tap boxes that readily connect to the output of a portable generator in the event of primary generator issues.

Overall Network Performance Management Efforts

The performance of Sprint's networks is monitored 24 hours a day, 7 days per week and 365 days a year by the Network Monitoring Centers. In addition, local switching offices staffed by trained technicians and management coordinate with these larger operations centers, to ensure that Sprint's networks are properly maintained.

Network Restoration Prioritization

Sprint's Business Continuity Management Team works as a customer advocate when large network outages occur. The team works closely with network recovery teams to establish customer prioritization once the backbone, TSP (Telecommunications Service Priority) and Critical Life Circuits are re-established. Sprint has an established cell site classification and service restoration process.

Special Event Planning

Special events have the potential for adversely affecting the customer experience due to greatly increased wireless traffic demands. Sprint has a mature special events process with dedicated project management personnel and a cross-functional management tool. Teams archive records of recurring special events and leverage capacity planning teams in implementing enhancements to optimize the customer experience. Sprint has used its experience in managing very large temporary users at NASCAR events to manage other special events. As an example, Sprint interfaces with the NCC (National Coordinating Center for Communications) in managing capacity needs at National Special Security Events, NSSE.

Sprint's Emergency Response Team (ERT)

The Sprint Emergency Response Team (ERT) is the first of its kind and was created in 2002. One of the industry's largest and most advanced disaster response programs, Sprint's ERT specializes in short-term, rapidly deployable, highly mobile and self-sustaining solutions that can provide critical communication and connectivity virtually anywhere, anytime. The ERT is an experienced, cross functional group, which consists of a national team of full time, dedicated personnel as well as over a thousand of ERT Reservists across the country.

Sprint ERT's innovative Rapid Deployment Solutions*1 provide an easily deployable and scalable set of voice, video, Sprint mobile data, hi-speed dedicated internet access, temporary managed Wi-Fi solutions and mobile devices to government agencies, public safety, the military, first responders, K-12 and University campuses, the healthcare community and private companies during declared emergencies, field training exercises, National Special Security Events (NSSE) and short-term special events. When either an emergency or planned event happens, Sprint ERT's rapidly deployable solutions seamlessly augment existing government or corporate communication infrastructures, working hand-in-hand with an agency or corporation's personnel and allows an entity to concentrate on vital operations instead of technical issues.

Sprint ERT Solutions

Sprint's ERT provides a comprehensive response to government and corporate critical communications requirements for cellular services, including 4G LTE, as well as Satellite IP/VSAT Services. Sprint ERT's Mobile Device and Satellite Solutions include the following:

- ERT Satellite Backhauled Cellular Voice, 4G LTE, and Satellite IP (VSAT) Solutions
  - ERT Satellite Cell on Light Trucks (SatCOLTs)
- ERT Satellite IP (VSAT) Solutions
- ERT Satellite Fly-Away-Kit (FAK)
- ERT Satellite IP Trailer
- Fixed Antenna and Customer Deployable Portable Solutions
- Multiple Contracting Options for Sprint ERT Satellite Solutions
- ERT Mobile Devices
  - ERT Go-Kits
  - ERT Rental Program
- ERT Professional Services

Satellite Cell on Light Trucks (SatCOLTs): Fully self-contained, mobile communication vehicles that offer cellular voice, push-to-talk and data services, as well as high-speed, mobile IP data services (wired and wireless) and can relay vital information over the Nationwide Sprint Network in remote areas.

ERT Go-Kit™: Provides government agencies and corporate customers instant access to temporary voice, Push to Talk, Data, Video, and other mobility applications. The Go Kit can include Sprint phones, Direct Connect devices, smart devices, tablets, mobile broadband cards, hotspots and critical accessories. Plans include a low monthly reservation fee with pay as you use service.

Satellite IP Solutions: Includes a Fly Away Kit (FAK), which is a portable auto-acquisition satellite package configured to ship either counter-to counter, commercial carrier or air transport. The FAK is offered as both a customer deployable solution or as a solution that can be maintained and deployed by Sprint ERT. Sprint ERT also offers fixed antenna systems designed to provide auto-fail over capabilities. Both FAK and permanently installed solutions can be

[1] **ERT services, product availability and pricing are subject to change at Sprint's sole discretion. Additional terms and conditions may apply.*

customized to contain a variety of client required equipment and configurations. Sprint satellite services provide coverage in the continental US, AK, HI, and PR with dedicated bandwidth speeds up to 40Mbps.

Professional Services: Available for inventory and life cycle management, planning, configuration, testing/exercising, network integration and technical support, and deployment and logistics management. ERT's dedicated team is comprised of industry, military and public safety veterans.

Sprint ERT also offers programming, training and technical support in a variety of areas. Agencies and corporations cannot tolerate a business continuity plan with a steep learning curve; it must work the first time an emergency tests it. Sprint’s ERT enables an agency or corporation to rest easily, knowing their solution is built with a robust, reliable, and tested program design where tasks are performed by Sprint ERT to avoid straining the agency or corporation’s resources.

Sprint’s Commitment to Public Safety through EOC Partnerships

Sprint is dedicated to maintaining contact with key Emergency Operations Centers (EOC) during major disasters and special security events. A process is in place for Sprint to support and communicate with state and county EOC's to help facilitate situational awareness.

Benefits of the EOC Information Sharing Partnership

- Sprint can respond to the EOC’s needs for recovery information and information sharing to facilitate situational awareness
- Obtaining critical information from the EOC that will aid Sprint in its recovery and restoral process (e.g. curfews or road closures for field restoration crews or generator deployment)
- Making key contacts within the EOC (EOC lead, utility representatives, other ESFs)
- Communicating EOC priority areas for recovery back to Sprint

Value of Sprint’s EOC Staffing Strategy for Public Safety

- Sprint is able to provide information and status updates to the EOCs on pertinent network recovery efforts
- The State EOC can provide direction on where *their* priority disaster areas are for Sprint to restore the network
- Sprint can obtain information from the other Emergency Support Functions such as ESF-12; Energy/Power that helps determine where to deploy our network recovery assets
- Proper credentials that allow our network technicians to pass through area access points that are otherwise restricted to the public
- Obtain locations of FEMA and other emergency responder command posts, to help Sprint plan for the influx of users/increase network capacity needs
- Overall, it is a way for Sprint to be proactive, not reactive, in the response and recovery efforts that may impact our communities

Contact Sprint’s ERT

For more information on Sprint’s Emergency Response Team, please visit us at:

- www.sprint.com/ert
- Become a fan on Facebook at www.facebook.com/SprintEmergencyResponseTeam
- Email us at ERTRequests@sprint.com
- Or contact our 24x7x365 ERT Hotline at 1-888-639-0020 (GETS users call 254-295-2220)

Large scale, natural and manmade events require reliable communications between all forces trying to ensure safety. The Sprint Emergency Response Team (ERT) helps to establish self-supported, interoperable mobile communications when agency and corporate networks are unavailable. For over a decade, Sprint ERT has supported short-term communication needs to first responders and corporations in emergency situations, large-scale exercises and major events. Sprint ERT Deployments include disaster situations, special event security initiatives, and field training exercises. Some recent deployments include the following:

Disasters

November 2013, Midwest Tornadoes

Situation: An EF4 tornado touched down in Washington, IL damaging nearly 500 buildings and resulting in one death and 125 injuries.

Sprint ERT Solution:

- Deployed a SatCOLT for additional bandwidth to the Illinois Emergency Management Agency
- Provided Sprint Direct Connect devices so the EOC could maintain contact with their volunteers
- Provided broadband connectivity to the Tazewell Joint Information Center (JIC) with Sprint ERT Fly- Away-Kit for dedicated satellite service

July 2014, Carlton Complex Fire Deployments Situation:

Lightning from a weather system created four fires in Washington State. These fires eventually grew into one larger fire that blew into the town of Pateros, consuming 300 homes and destroying critical infrastructure in its path.

Sprint ERT Solution:

- Provided satellite data via wireline and WiFi, cellular voice and Sprint handsets to improve communication between the Section Chiefs, Incident Commanders and teams helping fight the fire
- Supported ICP team members, over 2000 firefighters and Animal Response and Recovery team members

2013, San Juan Fiber Cut Deployment

Situation: A fiber optic cable was cut underwater between Lopez and San Juan Island. The cut impacted 911 services, emergency service agencies, the business community, wireless networks and 130,000 residents on Lopez Island.

Sprint ERT Solution:

- Deployed a SatCOLT for satellite backhauled hi-speed mobile IP services and 100 Sprint cell phones to support emergency services until the cut was repaired

October 2012, Hurricane Sandy

Situation: Hurricane Sandy caused power outages, flooding and wireless and wired networks to shut down on the shores of Southern New Jersey through New York up to the Western Great Lakes. Sandy left 8.5 million people without power, over 125 deceased and damages in the billions.

Sprint ERT Solution:

- Deployed portable VSAT solutions providing dedicated internet access for regional emergency operation centers
- Mobilized 13 SatCOLTs® from around the country for cellular and push-to-talk communications

- Delivered 5,800 Sprint handsets and mobile broadband devices and 250 tracking devices for fuel trucks to rescue efforts

October 2011, Hurricane Irene

Situation: Hurricane Irene was one of the most destructive hurricanes to ever make landfall in the United States and caused damages estimating in the billions and resulting in over 35 deaths.

Sprint ERT Solution:

- Provided more than 400 Sprint devices to dozens of first responders in local government and businesses from Florida to Maine
- Deployed SatCOLTS in three locations, utilizing on-board power and satellite backhaul to provide a private radio network for mobile communications

2011, Joplin Missouri Tornado

Situation: The Joplin, Missouri EF-5 tornado demolished parts of the city and ruined communication services.

Sprint ERT Solution:

- Provided short-term communications to the Joplin Joint Operations Center through voice services and IP connectivity
- Supported communication and connectivity in a regional hospital trauma center with push-to-talk devices and IP data services

April 2011, Alabama Tornadoes

Situation: The Alabama tornadoes caused significant damage in Huntsville and the surrounding area, impacting communication services in the Huntsville Hospital.

Sprint ERT Solution:

- Provided push-to-talk devices to the hospital to enable staff to maintain operations and coordinate the needs of patients across the community
- Used a SatCOLT to restore the hospital’s wireless communications
- Deployed a SatCOLT to provide coverage where networks were compromised or remote areas where there was no coverage

April 2010, West Virginia Mine Explosion Situation:

The topography and rural location of the West Virginia Mine Explosion caused limited communications coverage.

Sprint ERT Solution:

- Deployed a SatCOLT to provide a bubble of coverage to the rescue drilling operations
- Provided personnel and 100 rugged devices for communications support during the rescue operations

April 2010, Gulf Coast Oil Spill

Situation: The Gulf Coast Oil Spill was the largest oil spill in United States history. It required massive clean-up efforts including a Command Post, which hosted helicopter pads, a reconnaissance and information disbursement facility, buoy deployment and a repair and decontamination center.

Sprint ERT Solution:

- Deployed a SatCOLT and personnel at the Command Post to provide critical voice and data communications for the six-month clean up

3. Describe the types and amounts of back-up batteries, generators, COWs/GOATs and other deployable assets you maintain, and how long a period of disruption you anticipate in your planning.

ERT has an inventory of over 10,000 rental devices to deploy for clients requiring temporary, short-term voice and data solutions. All Sprint wireless services can be supported. Our ERT has an impressive and extensive track record with over 6,100 deployments and counting, over 700 public sector and enterprise agencies across the country, 40 presidentially declared disasters, and 11 national security events.

4. Also describe how your organization would continue to function in the event of a widespread environmental or health threat that would require most citizens to remain at home.

Sprint has matured its former "Pandemic Continuity" Plan into "employee continuity" plans which incorporate events that may result in employee injuries or fatalities or significant and sustained employee absenteeism. Examples include a pandemic or infectious disease that poses life-threatening risks to employees and their families, a company-owned building roof collapse, or an unplanned school closing due to a natural or a man-made disaster requiring parents to be absent from the work place. Sprint has a designated internal structure responsible for impact assessments and decision making during an employee continuity event as well as proactive planning to identify emerging threats and new strategy implementation. As Sprint's business continuity plans are developed with an "all-hazards" mindset, employee continuity strategies such as remote work, increased office cleanings and social distancing are considered in all plans.

3. 5G Cellular Services

Describe your deployment plans for 5G network coverage across the U.S.

Sprint was excited to be the first U.S. carrier to demonstrate elements of 5G at a large-scale public event such as the Copa América Centenario. Sprint's demonstration utilized 73 GHz millimeter wavelength spectrum to deliver peak download speeds of more than 2 Gbps. Showcasing a live streaming virtual reality system from VideoStitch that was highly responsive (with low lag) due to the low millisecond latency of the 5G system. In addition, spectators viewed live stream video in 4K ultra high-definition, displaying the blazing fast, high-bandwidth capability of 5G.

The 5G demonstration utilized beam switching, a method of tracking devices, selecting the best antennas, and sending their signals to targeted locations as well as Beamforming (used today in the Sprint LTE network) and beam switching. These are more efficient methods of sending signals in specific directions to improve data throughput and overall network reliability. The 5G system also included support for dynamic TDD – the ability to adjust in real-time the allocated capacity for downlink and uplink traffic based on network demand. In addition, Sprint also demonstrated how the 5G system would react to real-world obstructions such as various types of window panes.

As evidence of our commitment to make it happen, starting in April 2018 customers in Chicago, Dallas and Los Angeles began experiencing 5G-like capabilities, including significant increases in data speed and capacity, as Massive MIMO is rolled out. We will aggressively expand to additional markets including Atlanta, Houston and Washington, D.C. in late 2018. Sprint expects to deploy thousands of Massive MIMO radios, significantly increasing network capacity for millions of customers across the country.

As further evidence of our drive to be first to 5G, in mid-August, we announced that through our partnership with LG Electronics Sprint will be bringing the very first 5G phone to the U.S. in early 2019.

Sprint customers will be among the first in the world to have access to a true 5G smartphone. This device will have integrated 5G support and will not be clunky "bolt-on" solutions being developed by other carriers. Our first 5G product is a beautifully designed smartphone with a big OLED screen, triple-rear camera design and cutting-edge sound.

In a device, 5G will bring our customers a new level of speed, low latency and reliability that will help enable things like 8K video streaming, full-length HD movie downloads in seconds and new apps and services for augmented reality, virtual reality, mobile gaming and more. Sprint is moving fast on the road to 5G and we are thrilled to announce the first 5G smartphone. Additional devices designed for Sprint's new 5G network will be shared as they are announced.

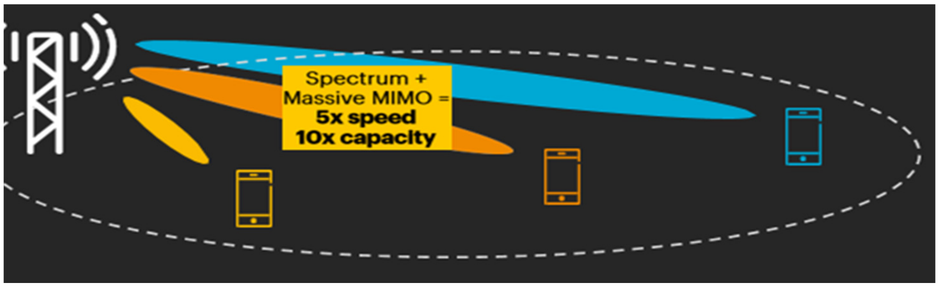
1. Expected Role of 5G in your overall network architecture.

Award-Winning 5G Strategy

We have a smart approach to 5G and are proud to share that Sprint has won a prestigious Leading Lights Award for "Most Innovative 5G Strategy." This industry award from Light Reading is important recognition of our use of 2.5 GHz and game-changing Massive MIMO technology to deploy 5G. The beauty of the technology is that it will dramatically increase the performance of our 4G LTE network, and when 5G is available, with a simple software update we'll be able to use the same radios to launch 5G.

It is important to point out that we developed Massive MIMO technology not just for 5G, but to enhance the performance of our 4G LTE network. With Massive MIMO in split mode, we are able to "kill 2 birds with one stone" and launch 5G simultaneously with LTE on the same hardware. We can pull this off because we are one of the few operators in the world with enough capacity to operate LTE and 5G on the same spectrum band (2.5 GHz). So, as we densify our network with more 2.5 GHz LTE, we can add 5G capabilities to the same cell sites, rather than having to build out our 5G network on entirely new sites or small cells.

Massive MIMO can increase network capacity up to 10 times that of current LTE systems.



2.

With our industry-leading spectrum portfolio, continued progress on our 4G LTE network and deployment of Massive MIMO technology as our bridge to 5G, we have a winning formula to ensure we deliver a great network experience for our customers and win the race to mobile 5G.

Other efforts to prepare the Sprint network for 5G include its network densification strategy, which enables Sprint to deliver high data rates even in crowded areas. Sprint is also in the process of deploying an NFV based Network

Core. This will allow Sprint to automatically, quickly, and easily expand and contract core elements capacity as required by the current loading on the network. This ability will help ensure a consistent user experience. The virtual core will also allow for the addition of new services and customer-required features in days instead of months.

We would like to understand where 5G "fits" in your overall network strategy. For example, do you see 5G as:

a. A wholesale upgrade for 4G LTE services in the wide area,

b. A high-capacity local distribution solution for a 4G wide area network,

b. Some combination of the two,

d. A fixed wireless solution for business or residential Internet access, or

e. Something else entirely.?

We believe 5G will enable new uses for mobile devices, with rate structures which will complement data-centric needs. Legacy networks weren't designed to handle the demands of the connected future. Ultimately connectivity, reliability, capacity, and coverage – virtually without limits and at massive scale –is the promise of 5G. While today's networks and devices are undeniably useful – with them we can book a flight, order a meal, and video chat with friends around the world – they are only the beginning of what will be possible with 5G. Entirely new levels of speed and latency will enable entirely new industries and business models to take place in the cloud. Extreme bandwidth and low latency will power highly immersive virtual reality experiences. And 4K and 8K video will be mainstream, with movie downloads in just the blink of an eye. Our smart cities, our methods of transport, and our homes will all be vastly different.

5G is being designed to support a variety of applications such as the IoT, Smart Cities, connected wearables, augmented reality, and self-driving automobiles. 5G will provide ultra-high-speed links for HD video streaming and virtual reality as well as low-data-rate speeds for sensor networks.

We know that future networks will need to be massively dense in order to meet the demand for higher data rates per person across a given geographic location. Practically speaking though, the requirements and building blocks for 5G are still being defined.

Sprint is positioned to be the first US carrier with true mobile 5G services. This capability will be built on our existing towers with new equipment that will provide 4G and 5G service simultaneously. We are also exploring the fixed high bandwidth services as well. Sprint is excited for all of the innovation that will occur, and we're proud to play our part in building the wireless platforms of the future.

3. Please provide the fundamental strategy you are following for deploying 5G technologies going forward.

Sprint's priority is mobile 5G, and the company is working with Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, and SoftBank to develop technologies for wide-scale 5G deployment. Sprint plans to provide commercial services and devices in late 2019. In addition, Sprint is working with its RAN (Radio Access Network) suppliers – Ericsson, Nokia, and Samsung – for end-to-end availability of 5G NR in Sprint's 2.5 GHz (n41) spectrum. Sprint's initial path to market for 5G will be through the deployment of 2.5 GHz Massive MIMO radios slated for commercial use in 2019. These 64T64R (64 transmitters, 64 receivers) radios will be software-upgradable to 5G NR.

Current planning efforts are more directed at further implementing advanced features of 4G LTE for transition to 5G, such as Massive MIMO (Multiple Input Multiple Output), 8T8R (8 Transmitter 8 Receiver), and Carrier Aggregation banding (2x, 3x, 4x) for maximum speeds eventually approaching 2 Gbps, as well as Voice over LTE (VoLTE) for a wireless unified-communications experience and small-cell deployment (network densification) for improved coverage in hard-to-reach locations and improved performance in locations with frequent spikes in traffic.

Sprint continues in a massive overhaul of network equipment (Network Vision). This overhaul enables not only the advanced 4G LTE services described above, along with improved capacity, coverage, and spectrum utilization; but it also future proofs Sprint's network infrastructure against standards and other change. Future upgrades, frequency changes, or even wholesale network standard changes in the move to 5G can likely be implemented with changes to software only.

To manage our 5G rollout Sprint has formed DEVGRU, a 5G advance team, charting Sprint's path to 5G deployment. This team will work closely with the network team, the device team, the marketing team, the product engineering team, the consumer and enterprise business units and others to make sure we are acting as one coordinated company to bring 5G to fruition.

4. Timetable and total percent of 5G coverage in each state.

In May we announced that New York City, Phoenix and our hometown of Kansas City have been added to our growing list of first 5G markets. These three markets join Atlanta, Chicago, Dallas, Houston, Los Angeles and Washington, D.C. as the first locations where we'll launch 5G in the first half of next year.

5. Proposed Channel Sizes (in MHz) for macro area and small cell deployments

Sprint has begun deploying pre-5G technology in the 2.5 GHz band on macro sites. This technology known as Massive MIMO will allow significant gains in capacity and performance over existing LTE services. The Massive MIMO radios will be software upgradeable to full 5G capability at a later time once 5G standards are complete.

Sprint's 2.5 GHz spectrum band is included in the Non-Standalone 3GPP 5G NR specification (initial part of Release 15) ratified at the 3GPP TSG RAN plenary meeting which is the core planning body for 5G deployment. The specification includes bandwidths up to 100 MHz for an n41 (2.5 GHz) single component carrier vs. today's 20 MHz per component carrier for 4G LTE. With more than 160 MHz of 2.5 GHz spectrum available in the top 100 U.S. markets, this gives Sprint the largest nationwide block of sub-6 GHz 5G spectrum available for wide-scale use in the U.S.

6. Frequency Band(s) to be used and primary applications for each.

Frequency bands are Band 25 (1900 MHz), Band 26 (800 MHz), Band 41 (2.5 GHz).

7. Pricing Model: Will 5G usage be metered and priced the same rates as 4G voice and data usage or will premium pricing be applied?

Sprint will continue to keep market rates competitive in the market. However, Sprint is not at a point in deployment to speak to expected rates for new 5G service.

4. VoLTE and Wideband Cellular Voice Services

Describe you plans for Voice over LTE (VoLTE) and Wideband voice services

Sprint currently provides simultaneous voice and data (SVD) through the use of an enhanced Wi-Fi calling service branded as Calling Plus. This service enables simultaneous voice and data service capabilities ahead of our VoLTE commercial deployment. The Calling Plus solution allows for VoIP call origination on the Sprint LTE network (LTE Calling), simultaneous voice and data services, and call continuity between Wi-Fi and LTE (Voice Call Continuity). Calling Plus is a free customer opt-in service leveraging the current VoWiFi infrastructure.

The base Wi-Fi Calling product is a free opt-in service that allows a user to access data while on a Wi-Fi voice call and is supported on both Android and Apple devices. Select Android devices support Wi-Fi calls for seamless hand-off to the Sprint Network (Voice Call Continuity); eliminating a call drop when Wi-Fi coverage is poor. A customer can use Wi-Fi calling at home, the office and at any public venue offering Wi-Fi data connectivity.

Wi-Fi Calling and Calling Plus minutes are free when dialing a US, US Virgin Islands, or Puerto Rico number. International rates do apply when dialing an international number.

1. Current level of VoLTE deployment and ongoing plans

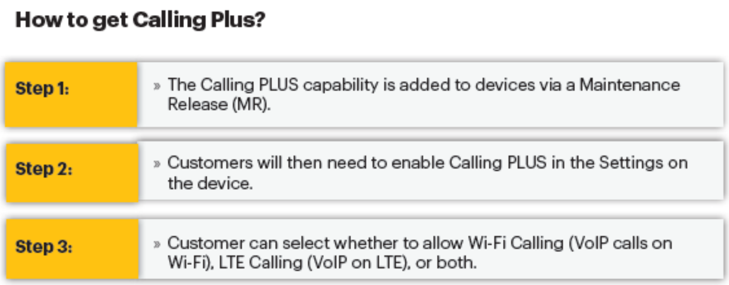
Sprint has enhanced our Wi-Fi Calling platform to offer the capability to use the Sprint LTE network for voice calls on select devices with Calling Plus. Calling PLUS allows VoIP call origination on the Sprint LTE network and seamless call continuity between Wi-Fi and LTE ahead of our VoLTE commercial deployment, which will provide simultaneous voice and data once it is fully launched. You can now talk, text and surf simultaneously. Get more done in less time!

Key Points:

- Voice Call Continuity (VCC) while moving between Wi-Fi and LTE
- Simultaneous Voice and Data capability (SVD) when in an LTE call
- FREE opt-in service integrated with the Wi-Fi Calling platform set up on initial activation
- Calling over the LTE network is added to existing voice calling option
- On-Device notification to inform users when Calling PLUS is being employed

Select Android devices support Calling PLUS, both simultaneous voice and data (SVD) and voice call continuity (VCC). VCC will support Wi-Fi initiated calls to be seamlessly handed off to the Sprint Network, eliminating a call drop when moving out of Wi-Fi coverage.

Wi-Fi Calling and Calling PLUS minutes are free when dialing a U.S., U.S. Virgin Islands, or Puerto Rico number. International rates do apply when dialing an international number.



How to get Calling Plus?

Step 1:	» The Calling PLUS capability is added to devices via a Maintenance Release (MR).
Step 2:	» Customers will then need to enable Calling PLUS in the Settings on the device.
Step 3:	» Customer can select whether to allow Wi-Fi Calling (VoIP calls on Wi-Fi), LTE Calling (VoIP on LTE), or both.

2. Wideband Voice (AMR-WB) Availability

Yes, it is available with the initial launch.

3. User device availability.

Select Android devices support Calling Plus.

4. Wideband Voice Interoperability:

- Between Mobile Carrier

Inbound and outbound roaming between Sprint and our partners is schedule to deploy at the same time as the rest of the VoLTE service.

- Mobile Carrier-to-PBX/UC Platform
(i.e. compatibility with wideband voice devices using G.722 or other wideband codecs)

This is supported today and will also with VoLTE.

5. Circuit Switched Fallback Included?

Yes, CDMA will remain generally available until we can migrate customers off of it and that's not likely to happen until early to mid-2020's.

6. Describe your overall pricing model for VoLTE services (e.g. Will wideband voice be offered at the same price as existing voice calling services?).

Domestic calls: Free and does not use plan minutes; International numbers.

a. Billed as normal; Data Usage for LTE Calls

b. Does not count toward any plan limits.

7. As "voice" has essentially becomes additional "data traffic" with VoLTE, indicate the likelihood you will be offering internet-like all-data plans that support all traffic types as opposed to plans that distinguish voice, data and text services.

Sprint will continue to work to offer plans with latest and greatest in technology. However, Sprint is not a position to speak to future internet-like all-data plans.

5. IoT Cellular Network Services

Describe what you currently have and plan to introduce in the way of network services specifically geared toward Internet of Things (IoT) applications.

The connected world of IoT will enhance businesses and the lives of people, and prove that there is more value from machines that are connected and communicating through a single big cloud. What started out as Machine-to-Machine communications has now evolved to the Internet of Things. The business world will greatly benefit from solutions that allow them to manage fleets, track assets, and enhance the shopping experience for Retailers. The advent of the Hours of Service mandate from the U.S. Government will increase opportunity for solutions Sprint already offers. These IoT solutions benefit all sorts of businesses, whether it is a big enterprise, a medium-sized business, or even a self-proprietorship. IoT delivers on its promise to either "Save Money" or "Make Money".

Sprint is the first mobile service provider to play an important connectivity role in the development of a U.S.-based Smart City ecosystem. In two Smart City tech workshops, Sprint, city officials, and other thought leaders shared best practices when deploying Smart Cities. The Smart City Tech summits featured Sprint's collaborative approach to teaming, reinforced our ability to customize IoT solutions for clients and allowed professionals to quickly meet leaders representing up to 25 cities throughout the nation.

One of the major challenges Sprint is addressing is IoT security. Phone hacking poses a very different threat than hacking a moving vehicle or a connected medical device and the consequences could be devastating. Hence, IoT security is a priority and the network of the future will be built on an architecture that supports an end-to-end security continuum. That's where our relationship with ARM Holdings the recent acquisition by Softbank our parent company will be of great importance. ARM employs a security technology called "TrustZone" that can clearly recognize and securely authorize devices on the network down to the hardware level. We are excited to work with ARM to bring new, differentiated and secure IoT products to market.

All of these things and more are possible, thanks to the Internet of Things. We are embarking on a connected world that is making lives better for companies and people every day.

1. **List all IoT-Focused Transport Services (e.g. NB-IoT, LTE Cat M1, etc.) Offered and Planned**

- CAT4 to CAT18
- CAT1
- CAT M1
- NB-IoT

2. **Performance Expectations (For each service offered):**

- Sprint CAT-1 is already launched and available on Sprint network.
- Sprint will be testing and deploying LTE CAT-M1 during 2018 with target of first commercially available network access planned for November 2018 with launch of new and dedicated IoT Core (Refer to press release on the following pages regarding dedicated IoT Core and OS). M1 will have variable rates up to 1Mbps using 1.4 MHz narrowband.
- NB will have variable rates in low 10s of kbps using 200 kHz narrowband.

- Uplink/Downlink Data Rates (Peak, Sustained, Cell Edge)

- Downlink up to 10Mbps, Uplink up to 5Mbps.

- Maximum Transmission Range

- Dependencies on topography and environment.

- Expected Latency

- Sub 30ms

- Frequency Band(s) Employed

- Bands 25, 26 and 41 for CAT1 through CAT18 and Band 25 for CAT M1 at launch of new IoT Core but will include Band 26 in future.

3. General Deployment Plans and Targeted Availability

- CAT1 to CAT18 (available today on existing core and RANs)
- CAT M1 (available on November 2018 with launch of dedicated IoT Core)
- NB-IoT (not yet planned but can be supported with existing RAN and new IoT Core design)

4. General Pricing Model(s) and Alignment To Minimize Cost with Specific Application Use Cases

Refer to Press Release on the following page.

Press Release

Sprint and Ericsson Reveal Ground Breaking IoT-Dedicated Core and Operating System

Fully dedicated, distributed and virtualized IoT core network works in tandem with the operating system to turn sensor data into immediate intelligence at the network edge; 5G-ready and primed for AI, robotics and more

OVERLAND PARK, Kan. – September 4, 2018 – Sprint (NYSE: S) and Ericsson have announced a global relationship to build a distributed and virtualized core network dedicated specifically to IoT (Internet of Things), in addition to a world-class IoT operating system. This new environment, which is purpose-built for the future of IoT, is designed to create an optimal flow of device data, enabling immediate, actionable intelligence at the network edge for end users and enterprises.

The global Sprint IoT platform is set to be presented at a press conference at Mobile World Congress Americas in Los Angeles, Wednesday, Sept. 12 at 10:30 a.m. (location: south hall, room 305).

"We are combining our IoT strategy with Ericsson's expertise to build a platform primed for the most demanding applications like artificial intelligence, edge computing, robotics, autonomous vehicles and more with ultra-low-latency, the highest availability and an unmatched level of security at the chip level," said Ivo Rook, senior vice president of IoT for Sprint. "This is a network built for software and it's ready for 5G. Our IoT platform is for those companies, large and small, that are creating the immediate economy."

"Sprint is a pioneer in IoT and we are excited to work together to create a truly disruptive IoT business," said Asa Tamsons, senior vice president and head of business area technology & emerging business, Ericsson. "Sprint will be one of the first to market with a distributed core network and operating system built especially for IoT and powered by Ericsson's IoT Accelerator platform. Our goal is to make it easy for Sprint and their customers to access and use connected intelligence, enabling instant and actionable insights for a better customer experience and maximum value."

Sprint + Ericsson: An Optimal Operating Environment for IoT
The two companies are disrupting the IoT world, creating an environment that is prepared for a future where society and business will be even more connected.

The Core Network:

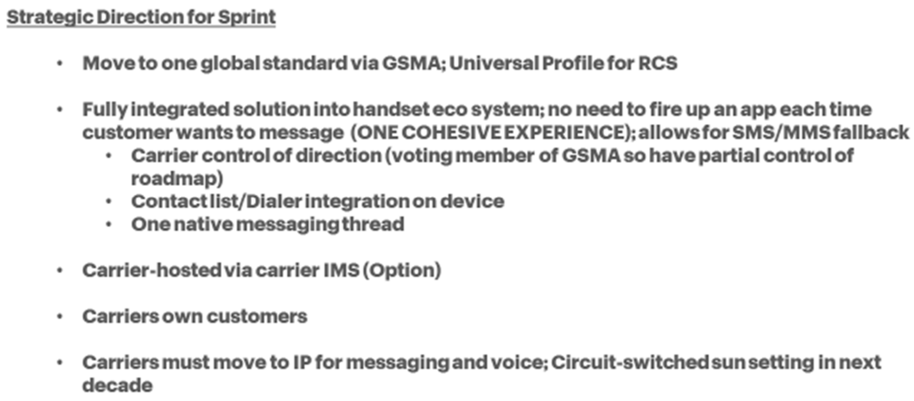
- **Dedicated to help provide:** low latency and highest availability.
- **Distributed and virtualized:** reduces distance between the device generating the data and the IoT application processing it; nodes are distributed right to the enterprise premise, if necessary, to support specific security, privacy and latency requirements.

The IoT OS:

- **Connectivity management and Device management:**
  - Capabilities enable simplified inbound and outbound activity for device connectivity.
  - Configuration and updates of firmware and software are managed for each device. All data is managed securely with world-class security on the chip level.
  - The IoT OS provides full subscription lifecycle management and monitoring of billing and usage data.
- **Data management:**
  - Capability to ingest enormous amounts of data while delivering immediate intelligence on that data.
- **Managed services:**
  - Service assurance for all IoT elements and enterprise locations, including network operations center monitoring, service resource fulfillment, cloud orchestration management and application management.

6. RCS Cellular Messaging Services

Describe your current and planned deployments of Rich Communications Service (RCS) service.



Strategic Direction for Sprint

- Move to one global standard via GSMA; Universal Profile for RCS
- Fully integrated solution into handset eco system; no need to fire up an app each time customer wants to message (ONE COHESIVE EXPERIENCE); allows for SMS/MMS fallback
  - Carrier control of direction (voting member of GSMA so have partial control of roadmap)
  - Contact list/Dialer integration on device
  - One native messaging thread
- Carrier-hosted via carrier IMS (Option)
- Carriers own customers
- Carriers must move to IP for messaging and voice; Circuit-switched sun setting in next decade

1. Planned/Deployed?

Sprint launched RCS (Rich Communications Services) in November 2016 on eight (8) Android devices. Almost all Android devices in 2017 and beyond will have RCS. iOS is not yet included in RCS.

2. Extent of Coverage

All carriers must move to IP as circuit-switched messaging (SMS/MMS) goes away in the next decade. Sprint must avoid becoming an island that cannot communicate with customers on other carriers. CDMA is being retired and equipment will eventually be phased out and finally not supported at a future date. Other carriers in the U.S. and world-wide are also deploying RCS which is the GSMA standard.

3. List of Features Offered

Sprint is partnering with Google to offer this service. Google provides the client, Android Messages as the default preload messaging client for android devices (non-Samsung). Google also provides the backend/cloud/IMS and the Google hub for interop cross-carrier. Carriers can build to the GSMA spec. or outsource the work. Google allowed Sprint to get to market quickly as well as the solution required almost zero investment. Samsung provides the RCS client on Samsung devices called Samsung Messages. Both apps can be updated or downloaded from Google Play. Samsung built their own RCS features into Samsung Messages which is the default messaging client on Samsung devices. Samsung uses the Google backend and hub. Features work when both users have RCS. When both handsets have RCS, then the customers can send via messages via IP, for example. If the downstream device does not have an RCS client, it is BAU and messaging will go via SMS, for example.

Upcoming Features: A2P (Business to Consumer) messaging (Example: American Airlines sending check-in info/boarding pass to device via IP message), BoTs that basically give RCS messaging a WAP experience feel within the messages vs. simply 160 characters today.

4. Supported devices

Sprint currently has about 3m devices provisioned with RCS and growing. This number will grow quickly as we launch each device. Initially customers saw an opt-in screen for the service however we are moving to auto opt-in going forward. Customers can toggle off RCS in the handset menu if they don't want to use it. Again, very similar experience to iMessage on iOS devices.

5. Expectations for user adoption going forward

RCS works between 2 clients that actively have RCS. RCS is an open standard so the implementation can be done by a carrier or service provider based on GSMA specs. RCS interop with not work with 3rd party applications like WhatsApp, Viber, Facebook Messenger, etc. If the message recipient does not have RCS, the message will fall back to SMS and deliver business as usual. RCS is a carrier grade implementation vs. customers using a 3rd party messaging application. Android Messages and Samsung Messages are the default messaging clients on our devices located in the hot seat on the device home screen. Apple is reportedly moving to adopt RCS for messaging that does not go between 2 iOS devices however the timeline is not yet established for their rollout.

7. Indoor Cellular Services

Describe your primary strategies addressing coverage problems in indoor or other difficult to service locations, and the type of support you can provide to our buyers in addressing these issues.

Sprint offers a variety of solutions to enhance voice and data in-building coverage. These solutions vary in capability, coverage and installation requirements. The Sprint Solutions Engineer will work with the customer to define the exact requirements and select the best solution. Below are several of the devices that Sprint can provide for voice and/or data coverage enhancement.

Sprint AIRAVE 3 LTE

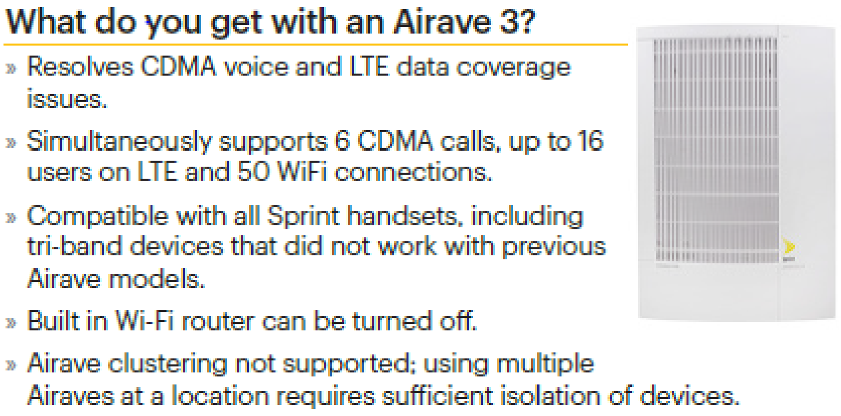
The Sprint AIRAVE 3 LTE provides dedicated coverage and capacity for CDMA voice, 3G (EVDO) and 4G LTE (Band 41) data services in a single device. AIRAVE is a femtocell, a personal base station with a radio unit similar to a cell tower radio. The femtocell uses a low-power antenna to transmit voice and data cellular signals for home or small office. Up to six simultaneous voice sessions and 16 data sessions are supported, enabling a small-medium office to take advantage of over 5,000 square feet of enhanced coverage. The AIRAVE 3 LTE can be deployed for work at home users or small office environments. The Sprint Account Team will work with the customer to qualify an AIRAVE 3 LTE opportunity.

Device Enhancements with AIRAVE 3 LTE include:

- 4G LTE Data support
- VoLTE ready
- Improved design with reduced size and integrated GPS puck

In addition the following existing AIRAVE functionality continues to be supported:

- Sprint-branded femtocell product designed to create a dedicated CDMA and 4G LTE signal within the home or office through your broadband Internet connection
- 3G EVDO/Rev A and 4G LTE Band 41 data coverage support
- Voice and data QoS built-in router prioritization
- Works to provide enhanced coverage for any 3G and 4G LTE Sprint devices
- Auto setup/Plug-N-Play
- Active hand-off coming from the AIRAVE and going to the Sprint Network (if a strong macro network signal is available)
- Has built in GPS which enables E911 location
- Private User Designation allows you to control who can use their AIRAVE 3 LTE



What do you get with an Airave 3?

- Resolves CDMA voice and LTE data coverage issues.
- Simultaneously supports 6 CDMA calls, up to 16 users on LTE and 50 WiFi connections.
- Compatible with all Sprint handsets, including tri-band devices that did not work with previous Airave models.
- Built in Wi-Fi router can be turned off.
- Airave clustering not supported; using multiple Airaves at a location requires sufficient isolation of devices.

Limitation:

AIRAVE 3 LTE does not support active handoff coming from the Sprint Network to the AIRAVE 3 LTE, also known as "hand-in". In this case, the phone will continue on the Sprint Network until the call ends. After the call ends, the phone will automatically lock on to the AIRAVE. However, when leaving the office, a call on AIRAVE 3 LTE will actively hand-off to the Sprint wireless network without any stoppage of the call in progress.

Customer Requirements

- High Speed Broadband Internet
- At least one active CDMA subscription on your account
- Strong macro network signal must be available for hand-off to work from the AIRAVE 3 LTE to the macro network – for location availability, please refer to www.sprint.com/airave.

Sprint NSC (S1000)

The Sprint Neighborhood Small Cell (NSC), also known as the S1000 provides dedicated coverage and capacity for 4G LTE (Band 41) data services and optional Wi-Fi in a single device. The S1000 is a femtocell, a personal base station with a radio unit similar to a cell tower radio. The S1000 is similar to the AIRAVE 3 LTE except that it is a **data only** small cell and does not support CDMA voice. The femtocell uses a low-power antenna to transmit 4G LTE data cellular signals for home or small office. Coverage is between 1,000 to 3,000 square feet and multiple S1000 devices can be installed in clusters for larger areas. Up to 14 simultaneous data sessions are supported per S1000.

Device Enhancements with S1000 include:

- 4G LTE Data support
- VoLTE ready
- Improved design with reduced size and integrated GPS puck

In addition, the following existing functionality continues to be supported in the S1000:

- Sprint-branded femtocell product designed to create a dedicated 4G LTE Band 41 signal within the home or office through your broadband Internet connection
- Works to provide enhanced coverage for any 4G LTE Sprint device that supports Band 41.
- Has built in GPS which enables E911 location

- Private User Designation allows you to control who can use the S1000

Limitation:

Only devices with Band 41 LTE radios can access the S1000.

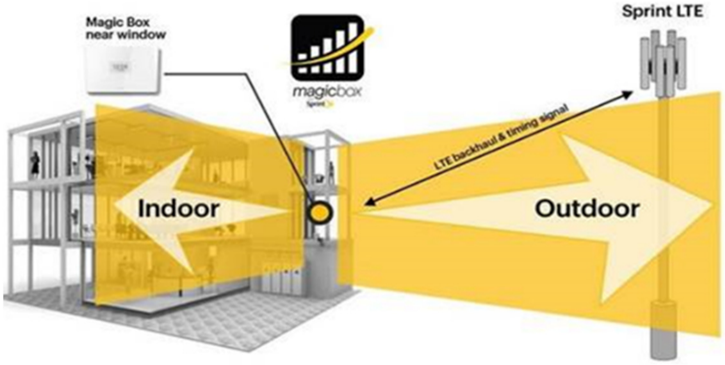
Customer Requirements

- High Speed Broadband Internet
- At least one active subscription on your account

Strong macro network signal must be available for data session hand-off to work from the S1000 to the macro network – for location availability, please visit: www.sprint.com/coverage.

Enhanced Micro Cell M2M Solution – Sprint Magic Box

Indoor coverage can be a challenge due to lack of signal penetration. To provide seamless coverage, Sprint has developed a plug ‘n play small cell technology that improves performance of the 4G LTE network. This unique solution is known as the Sprint Magic Box. Sprint’s Magic Box is a shoebox sized wireless femtocell relay device that is positioned on premise to increase signal strength in spectrum bands 41 and 25, and improve throughput of the Sprint 4G LTE Network. The Magic Box can enhance performance in areas up to 30,000 square feet, depending on environmental conditions like building construction.



Following are items included in the service:

- LTE+ small cell window booster
- High-speed data connectivity via Sprint 4G LTE network; **wireline web circuit not required**.
- Secure Wireless Ethernet bridge *(only included in qualified scenarios*)*

The equipment and service provided on premise is included (but standard data rates to apply to data used on Sprint mobile devices). For service to become operational, the Sprint small cell repeater must be correctly placed and plugged into AC power.

Sites that are potential Magic Box locations need to be validated to confirm that Magic Box will function at that address. The site(s) addresses can be sent to the Sprint Account Team for validation and confirmation of Magic Box service availability.

30,000 sq. ft. Indoor Coverage
100 Meters Outdoor Coverage

Coverage example within a commercial building and business

Features and Benefits

- **Plug-n-play deployment** - No engineering, construction or specialized labor required
- **Boosts Sprint's LTE signal and throughput** - Delivers enhanced signal and faster speeds
- **Enhanced Coverage** - Depending on site location and device placement, many sites will benefit from improved coverage and performance. Some locations may not need a Magic Box due to sufficient Macro Network coverage.

Flexible placement and operation

- Standard 110v outlet connection
- Draws only 35 watts in operation
- Typically deployed in any window
- Discreet deployment can be achieved via placement inside a lighted window sign

1. General technology approaches (e.g. DAS, small cells, indoor repeaters, VoWiFi, etc.) for different environments (Small office, large office building, campus, sports arena, etc.)

Sprint also offers a variety of Bi-Directional Amplifiers (BDA), BTS & DAS systems for very large building deployments to support voice and data. A BDA does not require customer provided backhaul but a BTS or DAS does require dedicated backhaul to the Sprint network. Mini-Macro's offering 800MHz or 2500MHz LTE are also available for large buildings where many users or floors need to receive enhanced in-building data coverage. Each large scale In Building Solution for voice and data must be approved based on cost and deployment timeframes. Sprint's In-Building Team will select the most appropriate solution to meet the need and work in conjunction with the site management and installation vendor to deliver these kinds of systems. Any coverage solutions requested by the Customer will be subject to: (i) Sprint's approval, which approval may be withheld in Sprint's sole discretion; and (ii) execution of a separate In-Building Solutions ("IBS") or Retransmission agreement with separate terms, conditions and fees, including, but not limited to, purchase of coverage solution equipment by the Customer, capital contributions, and/or purchase commitments.

These coverage solutions exemplify the kind of cutting-edge offerings Sprint provides to enable our clients to leverage investments in technology for tangible, real world results; reducing costs, eliminating capital expenditures, improving agility and providing exceptional responsiveness to their end users and customers.

2. Process by which states request assistance with special coverage issues.

States should initially contact your Sprint Contract Administrator and/or your Sprint local Government Account Manager to request assistance with special coverage issues. Your core Sprint team will collaborate with the states to define exact requirements and analyze needs to select the best solution.

3. Availability of guidance regarding suitability of specific solutions to particular applications, known tradeoffs, regulatory issues (e.g. retransmission rights), and potential interference with existing Wi-Fi or other unlicensed networks in operation.

Sprint sees emerging technology to leverage unlicensed spectrum as an opportunity for Sprint and it is complementary to our network strategy. While further evaluation is needed, we believe there needs to be co-existence between any unlicensed LTE technology, such as LTE-U or LAA, and Wi-Fi given the global ecosystem and extensive use of Wi-Fi in unlicensed spectrum today. Our focus is on providing quality service and service continuity regardless of whether our users are connected using our spectrum or using unlicensed spectrum.

While we continue to explore and test these emerging technologies for their potential to augment capacity and simplify network management, Sprint's massive spectrum reserves uniquely position us to support gigabit-class LTE – including more than 160 MHz of 2.5 GHz spectrum in the top 100 U.S. markets – for current and future carrier aggregation rollouts that will help us hit the 1 Gbps mark.

Your Sprint account team would provide further guidance and consultation as to these solutions and their suitability in support of your environment.

4. Special support services regarding coverage problems that will be available to NASPO ValuePoint users under this contract.

Coverage solutions vary in capability, coverage and installation requirements. Sprint has a portfolio of different solutions to help augment coverage and capacity that include WiFi Calling, bi-directional amplifiers (BDAs), and small cell products/ technologies that includes, but is not limited to, a shoebox sized wireless femtocell relay device that is positioned on a premise to increase signal strength in order to enhance performance in areas of up to 20,000 square feet, depending on environmental conditions (a solution referred to as the "Sprint Magic Box"). Any coverage solutions requested by the Customer will be subject to: (i) Sprint's approval, which approval may be withheld in Sprint's sole discretion; and (ii) execution of a separate In-Building Solutions ("IBS") or Retransmission agreement with separate terms, conditions and fees, including, but not limited to, purchase of coverage solution equipment by the Customer, capital contributions, and/or purchase commitments.

8. Cellular Services on Unlicensed Bands

Describe your overall plans for use of unlicensed frequency bands in providing your service, and how you intend to handle problems arising from customer private networks that are also using those channels.

Sprint will use whatever spectrum is necessary to provide the best service to their customers. Sprint already has sufficient spectrum with its Band 41 holdings for 4G and 5G deployments. Sprint can use additional available spectrum to ensure our customers have consistent experience; including unlicensed, lightly licensed, and additional licensed spectrum. The very wide bandwidth available in these bands will support extremely high peak data rates with very low latency. As unlicensed spectrum is shared, it cannot be counted on to always augment the customers' experience. For this reason, Sprint plans to use its licensed spectrum as the primary means to serve its customers.

Unlicensed spectrum is also used as an extension of connectivity to sensors and devices in Sprint's IoT solutions using a data aggregator. LPWAN, LORA, and Zigbee are examples of unlicensed spectrum technologies that have been used to create meshed networks of sensors through these aggregators.

1. Frequency bands being considered

Bands can include the unlicensed 5.8 GHz band, 3.5 GHz (CBRS), and mm Bands; mmBands are considered to be those frequencies that are above 24 GHz.

2. Planned applications for each band (e.g. Macro network, small cells, VoWiFi, etc.).

There is no plan on the macro network to use unlicensed spectrum for 5G.

3. What level of problems do you anticipate regarding interference problems created through your use of unlicensed channels that might be occupied by WLANs or other private wireless systems?

LTE/WLAN Aggregation, AKA: Radio Aggregation. LTE operates in the operator's licensed spectrum and Wi-Fi operates in the unlicensed spectrum. Co-located environment where LTE and Wi-Fi are directly linked, or in an environment which is not co-located where the eNodeB manages the internetworking between the LTE and Wi-Fi radio packets. This integration increases network capacity without having to make changes to the network core.

LTE-LAA: LTE operates in a carriers licensed radio frequency band **and** in the unlicensed 5GHz band. This technology utilizes LBT (listen before talk) technologies to minimize conflict with the local Wi-Fi signals. LTE-LAA enables the network operator to leverage the efficiencies of the LTE network core while simplifying user equipment architecture.

LTE-U: operates in both the network operator's licensed radio band and in the unlicensed 5 GHz band. However, this version would be implemented when LBT technologies are not required. This technology requires that "fair coexistence" between LTE and Wi-Fi radio signals exist. The specifications for this technology are currently being developed.

The Net

- Every Domestic U.S. carrier has committed to some implementation of the use of unlicensed spectrum
- Plans and specific Strategies are still in formation
- Primary implementation will be via the use of Small Cells or Distributed miniature Macro Antenna type equipment

Sprint is in a Unique Position

Sprint CTO John Saw: "though many carriers across the globe will "have to resort to" unlicensed technologies like Licensed Assisted Access (LAA) and LTE-Unlicensed (LTE-U), Sprint certainly isn't one of them."

Sprint plans to rely on its massive spectrum reserves – including more than 160 MHz of 2.5 GHz spectrum in the top 100 U.S. markets – for current and future carrier aggregation rollouts that will help it hit the 1 Gbps mark. High-band 2.5 GHz TDD LTE spectrum is uniquely suited for gigabit-class LTE.

4. How will users buying under this contract be notified that a system using unlicensed frequencies will be deployed in their facility and what steps will you be taking to ensure against interference with existing networks using those same unlicensed bands (e.g. Wi-Fi, Other 2.4 G/5GHz deployments.

Sprint continues to evaluate and test emerging technologies using unlicensed bands although they are under consideration as part of our long-term roadmap at the time of this writing. Sprint's CTO, John Saw, has emphasized the point in public statements that Sprint can achieve gigabit speeds without relying on unlicensed spectrum.

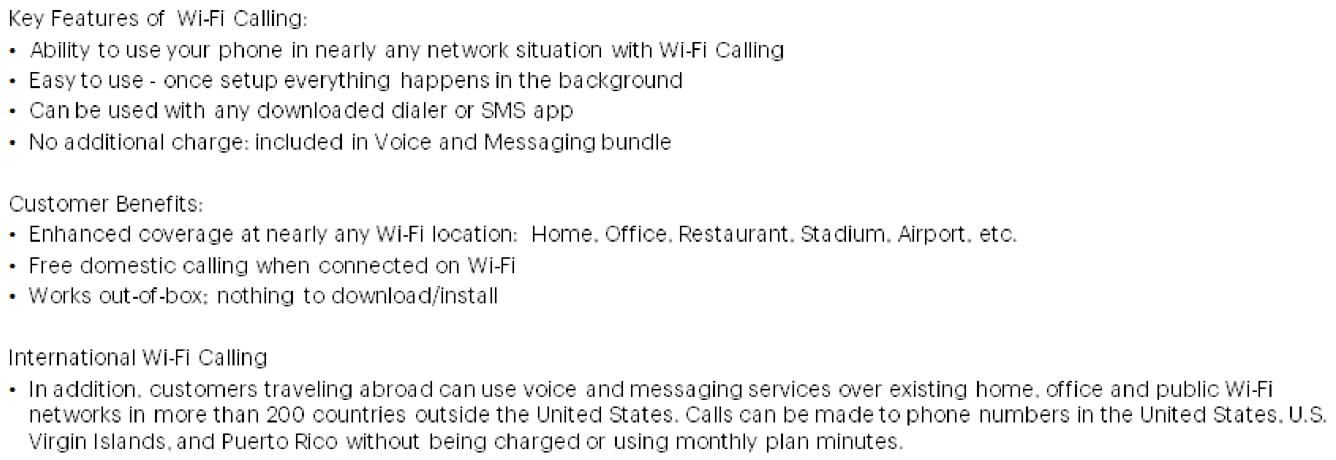
That said, we believe there needs to be co-existence between any unlicensed LTE technology, such as LTE-U or LAA, and Wi-Fi given the global ecosystem and extensive use of Wi-Fi in unlicensed spectrum today. We would anticipate deployment of any unlicensed technology to provide for the same quality service and our focus is on providing quality service and service continuity regardless of whether our users are connected using our spectrum or using unlicensed spectrum.

In early implementation, Sprint has produced some considerable performance results through use of LAA which is standardized and uses listen before transmit capabilities to co-exist with Wi-Fi. The small cell implementation also included Wi-Fi sensor capabilities to learn about the Wi-Fi environment it was operating within and adapt to changes in the Wi-Fi network to insure a high service quality. Once this technology becomes commercialized, it is to be expected that Sprint will strive for this same level of quality leveraging advanced technologies within the system to mitigate causes of interference with existing unlicensed systems such as those described above. In addition, Sprint account teams go to great lengths to insure customers understand our technologies and how they may impact existing customer environments as part of ongoing consultation, education, and updates.

9. Use of Wi-Fi in Cellular Services

Describe how you use Voice/Data/Text over Wi-Fi, the nature of the Wi-Fi services you would use, how the decision is made to use Wi-Fi versus cellular, and the impact Wi-Fi use will have on billable traffic.

Sprint provides Voice over Wi-Fi services. For our product name, Sprint refers as Wi-Fi Calling. Wi-Fi Calling functionality is embedded into select iOS and Android smartphones. Wi-Fi calling and International Wi-Fi calling (where available) is a FREE service for all Sprint customers with a supported device. Wi-Fi calling is currently available on select Apple**, Samsung, HTC, LG and Kyocera phones. Initial availability is via a software maintenance release with additional device updates as needed.



Key Features of Wi-Fi Calling:

- Ability to use your phone in nearly any network situation with Wi-Fi Calling
- Easy to use - once setup everything happens in the background
- Can be used with any downloaded dialer or SMS app
- No additional charge: included in Voice and Messaging bundle

Customer Benefits:

- Enhanced coverage at nearly any Wi-Fi location: Home, Office, Restaurant, Stadium, Airport, etc.
- Free domestic calling when connected on Wi-Fi
- Works out-of-box; nothing to download/install

International Wi-Fi Calling

- In addition, customers traveling abroad can use voice and messaging services over existing home, office and public Wi-Fi networks in more than 200 countries outside the United States. Calls can be made to phone numbers in the United States, U.S. Virgin Islands, and Puerto Rico without being charged or using monthly plan minutes.

1. Do you offload traffic onto Wi-Fi Networks?

Sprint leverages offloading to Wi-Fi networks in some scenarios such as offering free domestic Wi-Fi Calling to afford customers enhanced coverage at nearly any Wi-Fi location.

2. Indicate the approximate percentage of Wi-Fi usage for your total wireless network traffic over the following types of Wi-Fi networks:

- **Wi-Fi Networks built and maintained by you** **Voice _____ % Data _____ %**
- **Wi-Fi Networks from certified 3rd Party providers (e.g. Boingo, Cable Companies, etc.)-** **Voice _______% Data _____%**
- **Customer Wi-Fi Networks-** **Voice______ % Data______ %**
- **Any open and available Wi-Fi network-** **Voice______ % Data______ %**

Based on a third party study of the four major national carriers in 2018, approximately 70-80% of the monitored handset traffic used data over available Wi-Fi networks vs. cellular.

3. How is the service choice made to use cellular versus Wi-Fi, and which Wi-Fi network to choose if there are multiple options available?

Sprint devices are Wi-Fi preferred. This means that if the device has access to both cellular or WiFi, the device will use Wi-Fi for calls. This may change in the future to provide the user with a preference.

4. Are any of the following traffic types sent over Wi-Fi charged against the user's service plan?

- Voice?

No charges are incurred by the user's voice plan. Sprint does track WiFi calls separately and reports this information to the customer.

- Data?

No, Sprint does not have visibility to the amount of data sent over a Wi-Fi channel.

-Text (SMS/MMS)?

No, Sprint does not have visibility to the amount of text data sent over a Wi-Fi channel

10. Public Safety Wireless Priority Service (WPS) - For Bidders Offering Public Safety Services

Describe your ability to provide Wireless Priority Service (WPS) voice services for State employees with critical job duties and responsibility for responding to disaster/emergency events.

Stay connected when it counts. Even the best networks can get congested during a crisis. But when you're responding to a time-sensitive situation, every second matters.

That's where Wireless Priority Service (WPS) comes into play. WPS ensures that network congestion won't slow you down in an emergency. Sprint is an authorized provider of this service, which was created by the Department of Homeland Security to give critical voice calls a higher connection priority.

WPS works on a call-by-call basis. Users dial *272 and then the phone number. The voice call will then be prioritized and directed to the next available channel – without pre-empting any ongoing calls and without limiting the general public's use of regular networks.

WPS was designed to support entities that respond to various types of emergencies – where minutes or even seconds can make the difference between life and death. Typically these organizations are in charge of command and control efforts during the moments following a crisis or national security event.

If your organization falls into one of the following five priority categories, you can apply to the Department of Homeland Security for access:

Federal organizations can apply here. If you're a non-federal organization you can apply here.

Qualifying entities include:*

- Executive Leadership and Policy Makers
- Disaster Response/Military Command and Control

- Public Health, Safety, and Law Enforcement Command
- Public Services/Utilities and Public Welfare
- Disaster Recovery Agencies

Others who may qualify include security, education, critical infrastructure and emergency preparedness professionals.

As an authorized provider of WPS, Sprint provides fast, secure and dependable connections, even in an emergency. Refer to attachments regarding Wireless Priority Service and Priority Telecommunications Services uploaded for your review.

*WPS Customers require DHS approval for eligibility and level of priority. WPS prioritizes voice calls while on the Sprint network and roaming (if supported by roaming carrier). A specific calling code must be entered prior to the destination phone number to apply WPS prioritization. WPS Limitations: WPS calls receive priority over normal wireless voice calls, but are not guaranteed and do not preempt calls in progress or deny the general public's use of a wireless network. WPS calls are subject to wireless coverage and service limitations. Calls to 911 using WPS calling will be blocked. In the case of an emergency, customers should dial 911 directly. Other Terms: Coverage not available everywhere or for all phones/networks. Restrictions apply. See your Sprint Rep for details. Sprint. All rights reserved. Sprint & logo are trademarks of Sprint. Other marks are property of their respective owners.

1. Describe the general mechanism by which the network will prioritize WPS user calls (e.g. Will public network voice calls in progress be terminated to allow WPS calls to be connected?)

Enhanced Priority Treatment. Voice and Data (*) services supporting NS/EP missions will be provided preferential treatment over other traffic.

NGN WPS Voice Priority Services will have preferential access to resources and will use those resources on a preferential basis. Preferential treatment will be defined as treatment above and beyond the access, handling, and processing of communications services offered to normal entities and ordinary individuals. The priority status of the communication will be maintained for the total duration of the interaction (call, session, etc.). NS/EP Priority Services carriers will provide priority treatment to traffic marked with the NS/EP indicator—code point or a functional equivalent—when received from another authorized NS/EP Priority Services carrier. NGN Priority Services will also pass such indicators to subsequent connected network(s). For WPS wireless calls, NGN Priority Services will also convey the priority level from the access side to the egress side when transiting a Sprint's network between two wireless networks.
**Data priority services are in future planning stage under the DHS/OEC service offering and not currently available, however Sprint First Responder program may offer a service feature in the future.*

2. Can public safety officials disable calling for the general public to ensure WPS access for first responders?

Currently there is no voice call preemption, this may change in the future if government requirements are updated.

3. What happens when a base station or other network element becomes overloaded with WPS calls?

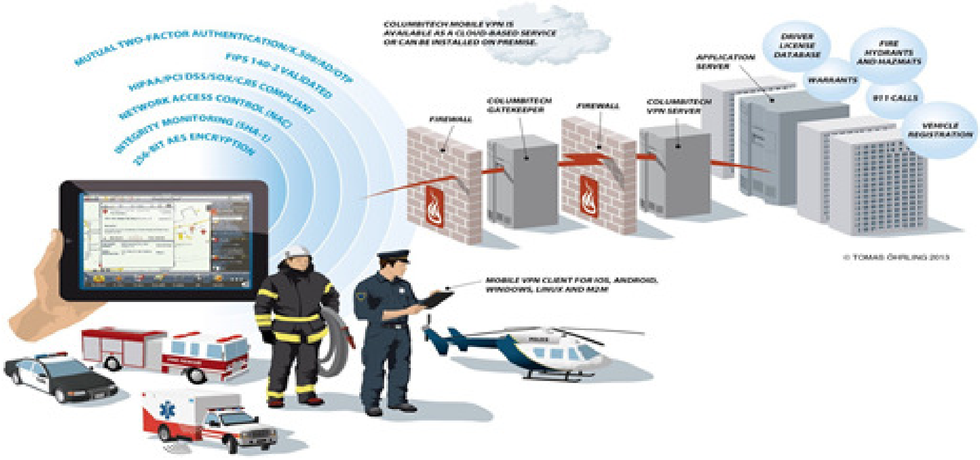
The caller will be queued for next available resource under these conditions. A caller experiencing a queued condition should remain on the line until the next available radio/network resource becomes available. WPS works on a call-by-call basis. Users dial *272 and then the phone number. The voice call will then be prioritized and directed to the next available channel – without pre-empting any ongoing calls and without limiting the general public's use of regular networks. WPS was designed to support entities that respond to various types of emergencies – where minutes or even seconds can make the difference between life and death. Typically these organizations are in charge of command and control efforts during the moments following a crisis or national security event.

In addition, **Sprint Secure VPN to** offer a Mobile VPN session persistence application that can run on any device OS (Apple, Android, Windows, Linux) via any network (LTE, Wi-Fi, or proprietary) and will automatically switch networks to ensure uninterrupted connectivity for critical law enforcement and/or first responder situations.

Sprint has partnered with Columbitech to offer Sprint Secure Mobile VPN is a security software solution designed for wireless networks. It creates a secure tunnel between a mobile device and the agency's network by using FIPS 140-2 validated end-to-end encryption in compliance with the Criminal Justice Information Services (CJIS) policy for law enforcement agencies. It uses two-factor (2F) authentication wireless technology to connect to federal, state and local systems.

The key to the Sprint Secure Mobile VPN application is the unique session persistence capability which securely monitors your connectivity, enables automatic roaming between networks and creates a continuous secure connection between the mobile device and the application server. Should connectivity be interrupted, the mobile VPN automatically reestablishes the connection so that users do not lose data or have to re-authenticate and restart applications when the connection is reestablished. The Sprint Secure Mobile VPN Application provides:

- FIPS 140-2 Certification and CJIS-compliance – Enabling you to meet federal regulations
- Advanced 2F Secure Authentication – Providing strong data security
- Continuously Monitored Session Persistence – Ensuring connectivity via variable networks
- Multi-OS platform support – Allowing you the flexibility to use virtually any device
- Handles all your secure data
  - 911 Calls, Warrants
  - Vehicle registration
  - Driver's license information
  - Surveillance camera and video
  - Fire hydrant and Hazmat maps


MUTUAL TWO-FACTOR AUTHENTICATION/X.509/AD/OTP
FIPS 140-2 VALIDATED
HIPAA/PCI DSS/SOX/CJIS COMPLIANT
NETWORK ACCESS CONTROL (NAC)
INTEGRITY MONITORING (SHA-1)
256-BIT AES ENCRYPTION
COLUMBITECH MOBILE VPN IS AVAILABLE AS A CLOUD-BASED SERVICE OR CAN BE INSTALLED ON PREMISE.
FIREWALL
COLUMBITECH GATEKEEPER
FIREWALL
COLUMBITECH VPN SERVER
APPLICATION SERVER
DRIVER LICENSE DATABASE
FIRE HYDRANTS AND HAZMATS
WARRANTS
911 CALLS
VEHICLE REGISTRATION
© TOMAS ÖHRLING 2013
MOBILE VPN CLIENT FOR IOS, ANDROID, WINDOWS, LINUX AND M2M

4. Define the range of devices supported.

All voice capable devices are supported, work is currently in progress for the support of WPS on VoLTE/VoWiFi. For devices that are CDMA and VoLTE, the service currently will work on CDMA. No data only devices are supported, so service not eligible for Tablets, modems, base stations etc.

Sprint has partnered with Columbitech to offer a Mobile VPN session persistence application that can run on any device OS (Apple, Android, Windows, Linux) via any network (LTE, Wi-Fi, or proprietary) and will automatically switch networks to ensure uninterrupted connectivity for critical law enforcement and/or first responder situations.

COLUMBITECH

5. Does the service operate on 2G, VoLTE, or both?

Currently the service works on CDMA voice with work in progress for future functionality on VoLTE and VoWiFi.

6. Do you provide enhanced reporting to public safety agencies regarding WPS availability, dropped calls, performance, etc.

Sprint Federal Operations provides WPS specific reporting to DHS/OEC who manages the priority service amongst the participating carriers. Sprint customers receive their business as usual billing. Sprint customer care may have access to provide customers inventory reports of the wireless devices/services. Sprint Federal Operations could provide a report that only confirms the list of devices on a customer account provisioned with the WPS service, but reporting would be limited to that feature only.

7. Describe the type of back-up and recovery measures that are included as part of WPS.

The Wireless Priority Services feature is available via approval from DHS/OEC. It is a calling feature managed via the participating authorized carriers. Sprint may have back-up and recovery services available but are not necessarily part of the WPS feature. So this would need to be addressed by Sprint.

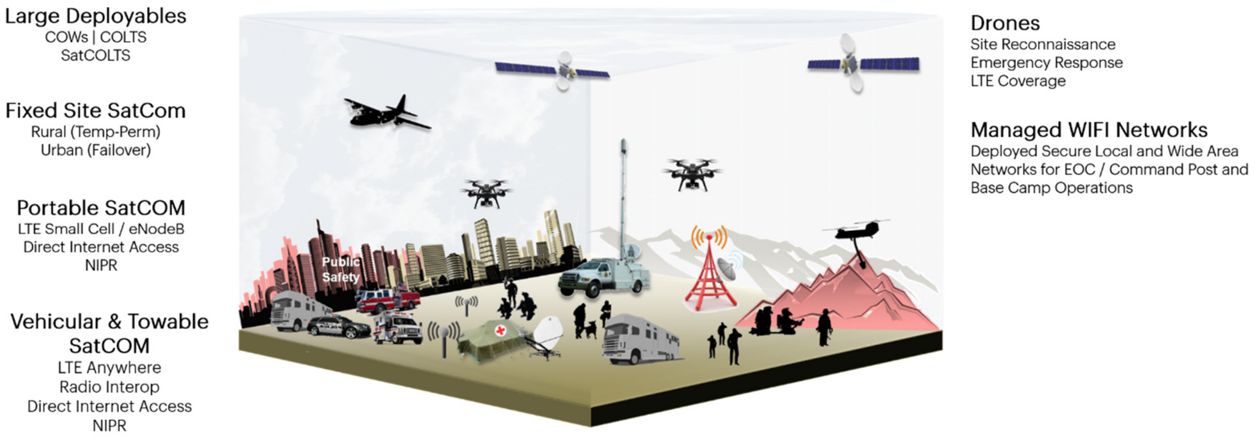
8. Do you have the ability to augment coverage/capacity with deployable assets during events/disasters?

Yes, during events or disasters, Sprint will deploy via the Emergency Response Team (ERT) assets in the recovery efforts. Fortifying Emergency Response Plans for our Public Safety customers is paramount at Sprint, and a function we have practiced for over 17 years. Sprint takes a two-pronged approach to Disaster Recovery and Emergency Response, insuring communications are available for Public Safety, no matter the event, no matter the location, and no matter the time. Sprint's Network Recovery and Emergency Response teams work in close collaboration with Public Safety and Government officials. Respectively, as a utility responsible for restoring and recovering the Sprint network, and as a mission assigned, support element (commonly in coordination with ESF2) with dedicated deployable assets and human resources in support of agency operations.

EMERGENCY RESPONSE TEAM: Sprint offers an additional layer of support the County's Emergency Operations Plan. In DIRECT support of and coordination with Miami-Dade operations (and similar to a mutual aid resource), Sprint's Emergency Response Team focuses on the development, implementation, and integration of "mission ready" communications assets, capabilities, and resources. Each Mission Assignment Request will be processed much like state and jurisdictional Mutual Assistance requests.

Of significant note, in a no-notice event, ERT national caches of deployable assets are designed to be deployed and operational anywhere in the continental U.S. within 48 hours, and in many cases less than 24. This requires an extraordinary amount of planning and practice internally and more importantly, externally in collaboration with state planners and leaders. For notice events, ERT will work closely with the agency to establish appropriate plans for staging of assets and resources to affect the most efficient and timely response to emergency events.

ERT deployable infrastructure assets are built on a concept of addressing and mitigating the varying issues that pertain to the loss, impairment, or lack of communications including power, backhaul, congestion, and access and take significant consideration into the varying environments in which they must operate. ERT Infrastructure assets are then further developed to be interoperable across a wide array of communications technologies spanning both Wireless, Wireline, and Land Mobile Radio systems, and in nearly any environmental setting including urban, rural, and remote, whether necessary for indoor or outdoor applications.



Sprint ERT's innovative Rapid Deployment Solutions* provide an easily deployable and scalable set of voice, video, mobile data, hi-speed dedicated internet access, temporary managed Wi-Fi solutions, and mobile devices to government agencies, public safety, the military, first responders, K-12 and University campuses, the healthcare community and private companies. When either an emergency or planned event happens, Sprint's ERT Rapid Deployment Solutions seamlessly augment existing government or corporate communication infrastructures, working hand-in-hand with ITS personnel and allowing your entity to concentrate on vital operations instead of technical issues.

Sprint ERT Rapid Deployment Solutions also offer programming, training and technical support in a variety of areas. Sprint's ERT Rapid Deployment Solutions enable you to rest easily, knowing your solution is built with a robust, reliable, and tested program design where tasks are performed by Sprint ERT to avoid straining ITS resources.

Sprint's Deployable Solutions provide a comprehensive and dedicated response to government and corporate critical communications requirements:

- Sprint Cellular Voice
- Sprint 4G LTE (5G available upon market launch)
- Sprint Direct Connect Plus
- Land Mobile Radio and Multi-Media Interoperability
- Communications Command and Control Interface
- Direct Internet Access
- ERT Mobile Devices
- ERT Professional Services

ERT Cellular Voice, 4G LTE & Satellite IP (VSAT) Solutions: Satellite Cells on Light Trucks (SatCOLTs)

In areas where both wireless and terrestrial infrastructure is impaired, non-existent, or simply needs augmenting, Sprint ERT can provide rapidly deployable, highly mobile and self-sustaining cell sites and mobile IP services.

The Sprint ERT SatCOLT (Satellite Cell on Light Truck) is a **mobile** communications vehicle offering cellular voice, Push-to-Talk (PTT), mobile broadband services, 4G LTE and high speed, satellite mobile IP data services (wired & wireless). The SatCOLT is capable of enhancing communications in an existing Sprint service area or provide service in a remote region where there is no existing infrastructure.

The Sprint SatCOLT provides connectivity through its satellite backhaul between the end user device and the Sprint network. Through this connection, end users can connect to any destination across the wireless network or PSTN. Additionally, with up to 40Mbps data throughput on a single vehicle, the SatCOLT can support LAN/WAN remote networking capabilities through its Satellite IP capability and Sprint's Global IP backbone.

The SatCOLT is **fully self-contained**, transportable both over-the-road and via air, and is deployed by a dedicated Sprint ERT strike team. The SatCOLT is built on a Ford F650 Super Duty chassis, includes a 65' telescoping mast, a 15kw generator, 160 gallon diesel fuel capacity and a 1.8M Ku satellite dish. The SatCOLT is air certified for C17 and above.

The Sprint SatCOLT is designed to be self-sustained over an approximate 5 day period based on actual usage and environmental conditions. In order to provide sustainable services over a period of more than 72 hours, Sprint employs a nationwide network of portable generators and multiple, national re-fueling contracts.

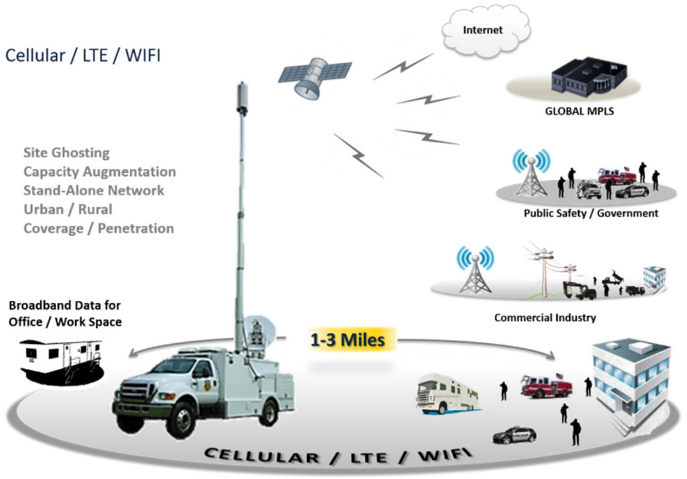
Interoperability: Disasters are unpredictable and even recent lessons from Harvey, Irma, and Maria illustrate this for notice events. Predicting which agencies will be required to support an event and with whom to communicate is only useful when events are fully controlled. Unfortunately, that paradigm exists only in perfect situations. As events unfold, the operational environment changes resulting in scaling complexity to the communications plan including with whom one must communicate as well as with what information must be accessed and shared. Through its integrated Mutualink® Interoperable Response and Preparedness Platform™, Sprint deployables can provide immediate resources to interconnect people, systems, and networks including LMR, PoC (Push to Talk over Cellular), Data, and Video.

SatCOLT Features:

- Backhaul:
  - Primary: Sprint's Satellite Network
  - Optional: Terrestrial Ethernet or Fiber and Microwave
  - Connected to the national Sprint network and MPLS, ESS & SprintLink network

- Services:
    - Sprint CDMA Cellular
    - Sprint Direct Connect Plus (MCPTT)
    - 4G LTE, 3G EVDO, and 1XRTT Mobile Broadband
    - Satellite IP Data - up to 40Mbps
- **Interoperability**
    - Integrated Mutualink Interoperable Response and Preparedness Platform
    - Radio Network Interface
    - Video Network Interface
    - Mutualink EDGE®
    - Local and Remote access
    - Distributable over WIFI or LTE
- **Vehicle**
    - F650 Super-Duty Chassis
    - 22K GVW
    - 305"L x 102" H x 97 W
    - Certified Air Transportable
    - Fully air conditioned
    - Auto-leveling
    - GPS navigation
    - 160 gallon on-board fuel
    - 15kw diesel generator w 180gal aux
- **Coverage**
    - 1-3 mile cellular (unobstructed)
    - ½ mile Wi-Fi (output, unobstructed)
- **Subscriber Support**
    - Cellular
        - ~1,800 subscribers
        - ~450 simultaneous voice
    - IP Data
        - minimum 50 per SatCOLT / VSAT terminal

Typical SatCOLT Deployment Scenarios



ERT Satellite IP (VSAT) Solutions

Sprint ERT's Satellite IP solutions provides secure voice/video, hi-speed dedicated internet access and temporary managed Wi-Fi services (LAN/WAN, VoIP, VSAT, Wireless Access Points, Scalable number of users). Satellite IP solutions focus on providing temporary Joint Field Office operations. Sprint's ERT can provide custom infrastructure quotes based on the County specifications to build satellite IP Infrastructure that is leased for extended periods or on an event-by-event basis for remote or capacity needs. Additionally, Sprint's ERT can provide both temporary and permanent wireless voice and data communications solutions for requirements outside the continent of the United States (OCONUS).

Sprint ERT leverages multiple infrastructure platforms to offer customized solutions to meet individual organizational needs. Satellite IP systems offer highly mobile, scalable, dedicated space segment up to 40Mbps, 100% CIR, in either symmetric or asymmetric configurations, with either dynamic or static IP addressing schemes. Our deployable and fixed communication systems provide immediate broadband connectivity via its secure, IP-enabled satellite network. This accessibility supports a wide array of IP-based applications including backhaul for Small-Cell deployments, Dedicated Internet access, VPN tunneling, VoIP and RoIP, as well as streaming video and audio for complete business operations and situational awareness support. Furthermore, ERT extends its IP service capabilities with multiple options for connectivity including, Ethernet, Fiber, and secure Managed Temporary Wi-Fi Mesh. Temporary Mesh networking options include both low-density and high density LAN/WAN applications.

ERT Satellite IP (VSAT) Solutions: ERT Fly-Away-Kit (FAK) & Satellite IP Trailer Deployable Satellite Solutions Infrastructure (VSAT)

The ERT Fly-Away-Kit (FAK) and Satellite IP Trailer provide fast, secure satellite communications via a KuBand satellite dish to provide quick access to data, Voice over IP (VoIP) and video teleconferencing at almost any location in the United States. Both solutions are designed to be easily transported and deployed.

Type 1 encryption is offered as an additional feature. No commercial power is required for the IP Trailer configuration, as an on-going generator can power up internal and external equipment. Both systems are deployed by a small Sprint ERT strike team and designed to require minimal participation or support from the County personnel. Features include:

- MOU / Assurance / Dedicated Contract Options
- Up to a 2.4 Meter dish
- Comtech 625 or 750 Modem Package
- Ku Band Satellite Service
- Full Redundant Satellites and Earth Stations
- Minimal on-site set-up (typical < 1 hour)
- Up to 40 Mbps of bandwidth
- Can include solution for remote/limited cellular integration
- Dedicated Space Segment (Bandwidth)
- Asymmetric / Symmetric Bandwidth Options (symmetric only over 10Mbps)
- Dynamic / Static IP Addressing
- VLAN Tagging

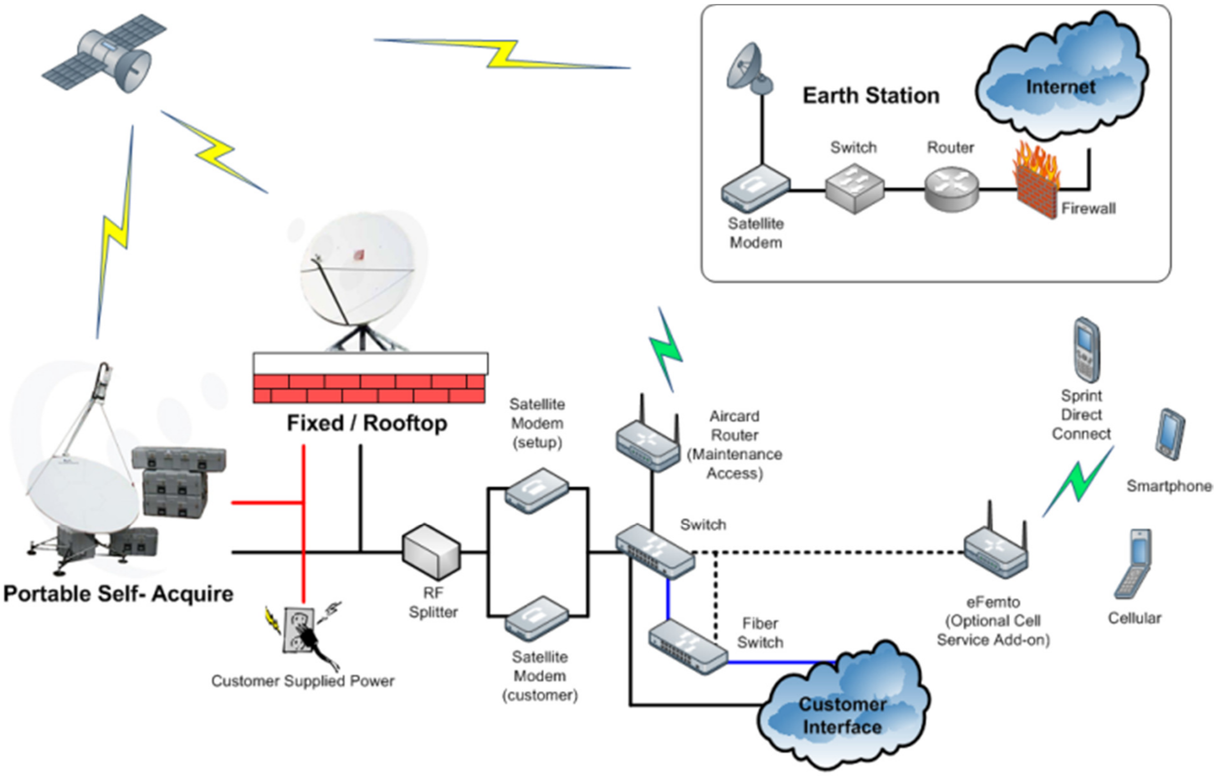
ERT Satellite IP (VSAT) Solutions: Fixed Antenna and Customer Deployable Portable Systems

Fixed Antenna Systems and portable Satellite Solutions from Sprint provide all the benefits of high speed dedicated internet access, without the constraints and dependencies of terrestrial networks. Whether it's providing robust diversity or moving the connection anywhere, anytime, you can rely on Sprint to keep you connected.

Whether you need access to basic office applications or need to support higher-bandwidth requirements for video and telemedicine, Sprint ERT offers a host of customized and configurable solutions.

- Purchase / Lease to Own Options for Portable Systems
- Always-On Bandwidth Pricing with Pay As You Use Billing Options
- Ku Band Satellite Service
- Redundant Satellites
- Redundant Earth Stations (Franklin, NJ and San Ramon, CA)
- Minimal on-site set-up (portable)
- Configurable solutions up to 40Mbps for fixed systems
- Dedicated Space Segment (Bandwidth)
- Asymmetric / Symmetric Bandwidth Options
- Symmetric only over 10Mbps
- Dynamic / Static IP Addressing
- VLAN Tagging
- Full suite of professional services
  - Dedicated Program Management (included)
  - 24x7x365 Dedicated Call Center (included)
  - Optional On-Site Technical and Network Support (fee based)
  - Exercise Support (fee based)

Typical ERT Satellite IP (VSAT) Solutions Deployment



NETWORK RECOVERY: To augment the capabilities of our ERT, Sprint's Network Recovery team utilizes a nationwide fleet of deployable assets and resources, including but not limited to Cellular site on Wheels (COW), COLTs, Repeaters, Portable Microwave Systems, and Portable Generators to restore network services when communications become impaired, congested, or otherwise unavailable. To the extent possible, the Network Recovery team in coordination with Sprint's Emergency Response Team, and Regional Network Teams, and assigned Agency Account Teams, will work with the agency to identify and act upon priority restoration requests.

Sprint has a very robust emergency response and disaster recovery plan which enables quick restoration of impacted services following a disaster. Sprint mitigates congestion risks through traffic management algorithms to handle the overload surges in traffic. Additionally, Sprint's well trained and exercised disaster recovery response teams proactively monitor congestion and performance of the wireless network and determine the appropriate course of action. This may include performing parameter changes, adding additional capacity to the network via radio installations to cell sites and/or by adding additional backhaul.

Cell Site On-Wheels (COW) and Satellite On-Light-Trucks (SatCOLT) may also be used to replace and/or expand Sprint's foot print or add additional capacity to the network. Sprint maintains a national fleet of COWS, COLTS, Portable Generators, Portable Microwave Systems, Satellite Cell on Light Trucks (SatCOLT), and other mobile assets ready to deploy anywhere within Sprint service territory.

The staging of Sprint's mobile infrastructure is developed during the activation of Sprint's Incident Action Plan (IAP). Sprint takes an all-hazards approach to Incident Management thus resource allocation and staging plans are based on each incident's unique threat analysis and information g with Public Safety each incident's potential unique characteristics and requirements. For disaster and emergency events, event specific Pre-IAP is developed no less than 72 hours prior to a notice event and immediately in response to a no-notice event. For non-emergency, planned events, IAPs may be developed as earlier as 18-24 months in advance, most notably for those that are designated as NSSE or of national significance. The IAPs are then correlated with the County's specific plan for that incident to insure seamless and efficient integration of Sprint plans and resources.

9. Detail levels of user priority defined and procedures required in applying for and initiating WPS for a user.

WPS is available only for authorized NS/EP users. The OEC has established five categories to identify critical NS/EP leadership functions and determine eligibility.

1. Executive Leadership and Policy Makers

Users who qualify for the Executive Leadership and Policy Makers priority will be assigned priority one. A limited number of wireless service technicians who are essential to restoring the wireless service networks shall also receive this highest priority treatment. Examples of those eligible include:

- The President of the United States, the Secretary of Defense, selected military leaders, and the minimum number of senior staff necessary to support these officials
- State governors, lieutenant governors, cabinet-level officials responsible for public safety and health, and the minimum number of senior staff necessary to support these officials
- Mayors, county commissioners, and the minimum number of senior staff to support these officials

2. Disaster Response/Military Command and Control

Users who qualify for the Disaster Response/Military Command and Control priority will be assigned priority two. Individuals eligible for this priority include personnel key to managing the initial response to an emergency at the local, state, regional and federal levels. Personnel selected for this priority should be responsible for ensuring the viability or reconstruction of the basic infrastructure in an emergency area. In addition, personnel essential to continuity of government and national security functions (such as the conduct of international affairs and intelligence activities) are also included in this priority. Examples of those eligible include:

- Federal emergency operations center coordinators, e.g., Manager, National Coordinating Center for Telecommunications, National Interagency Fire Center, Federal Coordinating Officer, Federal Emergency Communications Coordinator, Director of Military Support
- State emergency services director, National Guard Leadership, State and Federal Damage Assessment Team Leaders
- Federal, state and local personnel with continuity of government responsibilities
- Incident Command Center Managers, local emergency managers, other state and local elected public safety officials
- Federal personnel with intelligence and diplomatic responsibilities

3. Public Health, Safety and Law Enforcement Command

Users who qualify for the Public Health, Safety and Law Enforcement Command priority will be assigned priority three. Eligible for this priority are individuals who direct operations critical to life, property and maintenance of law and order immediately following an event. Examples of those eligible include:

- Federal law enforcement command
- State police leadership
- Local fire and law enforcement command
- Emergency medical service leaders
- Search and rescue team leaders
- Emergency communications coordinators

4. Public Services/Utilities and Public Welfare

Users who qualify for the Public Services/Utilities and Public Welfare priority will be assigned priority four. Eligible for this priority are those users whose responsibilities include managing public works and utility infrastructure damage assessment and restoration efforts and transportation to accomplish emergency response activities. Examples of those eligible include:

- Army Corps of Engineers leadership
- Power, water and sewage and telecommunications utilities
- Transportation leadership

5. Disaster Recovery

Users who qualify for the Disaster Recovery priority will be assigned priority five. Individuals eligible for this priority are responsible for managing a variety of recovery operations after the initial response has been accomplished. These functions may include managing medical resources such as supplies, personnel or patients in medical facilities. Other activities such as coordination to establish and stock shelters, to obtain detailed damage assessments, or to support key disaster field office personnel may be included. Examples of those eligible include:

- Medical recovery operations leadership
- Detailed damage assessment leadership
- Disaster shelter coordination and management
- Critical Disaster Field Office support personnel

Request via the NCS

Sprint cannot process WPS' requests. Below is the process for requesting WPS.

- ♦ Direct the customer to the National Communication System (NCS) to request WPS.
  - ○ Web site address: https://www.dhs.gov/wireless-priority-service-wps
  - ○ ○ Email: gets@hq.dhs.gov
  - ○ Toll free: 866-627-2255
  - ○ Direct: 703-676-2255
- ♦ NCS reviews the request and then assigns the priority level if approved.
- ♦ If approved, NCS will send to the Sprint Public Safety Care Support team (PSCC) for processing.
- ♦ Sprint Public Safety Care Support will establish and apply Sprint billing codes.

Delete or Unsubscribe to Wireless Priority Service

- ♦ Direct the customer to the National Communication System (NCS) to request to unsubscribe from WPS.
  - ○ Web site address: https://www.dhs.gov/wireless-priority-service-wps
  - ○ Email: gets@hq.dhs.gov
  - ○ Toll free: 866-627-2255
  - ○ Direct: 703-676-2255
- ♦ NCS reviews the request and then approves the customer to unsubscribe from WPS.
- ♦ If approved, NCS will send to the Sprint Public Safety Care Support team (PSCC) for processing.
- ♦ Sprint Care Support will remove WPS and expire any applicable billing codes.

Making a WPS Call

If a customer inquiries on how to make a WPS call once approved by the NCS and processed by PSCC:

- ♦ On the phone, dial *272 and then the telephone number.
  - ○ Example: *272 303-555-2222.

10. Confirm your ability to activate equipment and WPS within 24 hours after request in the event of a State of Disaster/Emergency.

WPS is available only for authorized NS/EP users. The DHS/OEC has established five categories to identify critical NS/EP leadership functions and determine eligibility. Ultimately, DHS/OEC has approval for use of the service feature as well as defining to the carrier the approved use level. Refer to above response for WPS user priority activation. Participating entities can contact their local sales or care representative with requests to activate equipment within 24 hours upon a State of Disaster/Emergency. Additionally, entities can contact our Emergency Response Hotline 24x7x365 at (888) 639-0020 for after hours' assistance.

11. National Broadband Public Safety Networks (NPSBNs) - For Bidders Offering Public Safety Services

Describe your plans for deploying FirstNet or FirstNet-like (i.e. National Broadband Public Safety Network) solutions for providing priority data and video service to State employees with critical job duties and responsibility for responding to disaster/emergency events.

Sprint is working towards deploying additional priority services capabilities on Sprint's public wireless network. Sprint will leverage QPP parameter assignment using the standard service control parameters defined by 3GPP and the Internet Engineering Task Force including Access Class, Quality Class Indicator (QCI) and Allocation and Retention

Priority (ARP). These capabilities will prioritize qualified users data traffic with critical job duties in the event of extreme network congestion during disaster/emergency events. Sprint is targeting mid-2019 availability.

Service Overview

1. **Will the priority NPSBN service operate over a fully separate radio access (RAN) and evolved packet core (EPC) network, and if not, what elements will be shared with the public wireless network. Are those plans expected to change in the foreseeable future?**

Sprint's deployment of the service for NPSBN will operate on Sprint's public wireless network. At present, Sprint does not have plans to deploy these services on a separate RAN or core network.

2. **In shared network elements, describe the specific mechanisms by which public safety traffic will be prioritized over other public network traffic in both wireless and wired portions of the network.**

Sprint will leverage QPP parameter assignment using the standard service control parameters defined by 3GPP and the Internet Engineering Task Force including Access Class, Quality Class Indicator (QCI) and Allocation and Retention Priority (ARP).

3. **Describe the range of capabilities available to support Quality of Service (QoS) for different classes of public safety traffic (e.g. voice, video, PTT/MCPTT, priority data, best effort data, background data, etc.), and what modifications would be required on end user devices or servers to mark traffic so that it would be assigned to the correct QoS priority level.**

Sprint will leverage QPP parameter assignment using the standard service control parameters defined by 3GPP and the Internet Engineering Task Force. Priority user traffic will be set a Quality Class Indicator (QCI) value and configurable by Sprint for qualified users. Modification to End User devices is not required.

4. **What radio frequency band(s) will your public safety service be operating on? Are there plans to change or expand that list?**

Public Safety users can operate on all Sprint's radio frequency bands. Certain capabilities like QoS are available on Sprint LTE bands as described above.

5. **At any point do you plan to offer a physically separate public safety RAN (please provide your definition of "physically separate") using Band 14, and will public safety officials have the ability to preempt access to those radio network resources from the general public in the event of an emergency or disaster?**

At present, Sprint does not have plans to deploy these services on a separate RAN or core network. Sprint is working towards offering the ability to give public safety officials the ability to preempt data access to radio network resources from the general public in the event of extreme network congestion. Sprint designs, deploys and maintains its public network to more than adequately support capacity demand.

6. **Describe the availability of compatible end devices for your public safety services, and identify any potential changes to your network offering (e.g. migration to Band 14) that would require device upgrades, and the scale of those upgrades (e.g. New SIM, Other hardware update, device replacement, etc.).**

Services will be available on Sprint LTE and Sprint VoLTE compatible end devices.

7. Does this page from the FirstNet Web Site <https://www.firstnet.com/devices>represent the complete list of FirstNet Certified Compatible devices?

Not applicable.

8. Describe what happens when all public network traffic has been preempted and the network becomes overloaded with public safety traffic.

Sprint services for public safety is deployed on Sprint's public wireless network. It would be a rare event to have all public network traffic preempted on the Sprint network due to congestion. In that unlikely event, public safety user traffic would be prioritized based on user priority level settings as defined in defined by 3GPP and the Internet Engineering Task Force. Priority. Public Safety users with higher priority designation would receive higher priority treatment.

Service Offerings and Performance Guarantees/Expectations

9. Voice Telephony: What are you plans, timetables and proposed technologies to offer wireless voice telephony services on your public safety network, and will it be carried with appropriate QoS?

Sprint offers Voice Telephony services to public safety customers on Sprint public wireless network. Please see Sprint responses to Wireless Priority Services responses as it relates to QoS.

10. Video: What are you plans, timetables and proposed technologies to offer wireless video services on your public safety network, and will it be carried with appropriate QoS? As video calls may be originated from a laptop, how will the user signal to the network that this is a video call so that appropriate QoS handling can be applied?

Sprint offers Video over Data services to public safety customers on Sprint public wireless network. Qualified public safety data traffic will be carried with appropriate QoS when available.

11. Broadband Data Performance Expectation/Guarantee:

- **How many levels of priority data services (e.g. Critical, High Priority, Best Effort, Background Data, etc.) will be offered, and how will user devices signal to the network the QoS level that should be applied to each session?**

  Sprint is working towards offering multiple levels of priority data services and targeting alignment with DHS WPS designation.

- **Uplink/Downlink Data Rates (Peak, Sustained, Cell Edge) and Latency for each QoS level supported.**

  Sprint is working towards offering multiple levels of priority data services and UpLink/DownLink data Rates are being defined.

- **Impact on network performance in Network Overload Conditions**

  Sprint employs a holistic approach to managing congestion on its data network. Sprint's first goal is to avoid congestion altogether by directing traffic to the best available spectrum resources and cell sites. Sprint also attempts to avoid congestion by managing tonnage on its network. Finally, when congestion does occur, meaning that the demand on a particular sector temporarily exceeds the ability of that sector to meet the demand, Sprint relies on the radio scheduling software provided by Sprint's hardware vendors to allocate resources to users.

- *Allocating Resources During Times of Congestion:* Despite our best efforts to prevent congestion through managing tonnage and directing customers to the best available network resources, the demand on a particular network sector sometimes temporarily exceeds the ability of that sector to meet the demand. During these times, Sprint relies on the radio scheduling software provided by Sprint's hardware vendors to allocate resources to users. This radio scheduling software includes a set of generic fairness algorithms that allocate resources based on signal quality, number of users, and other metrics. These algorithms are active at all times, whether or not the cell is congested; however, during times of congestion, the algorithms operate with the goal of ensuring that no single user is deprived of access to the network.

- *Real-Time Traffic Management System (RTTMS):* Another tool Sprint has deployed to help improve the customer experience for the majority of customers during times and places where network resources are constrained is Sprint's RTTMS. When a Sprint site is resource constrained, RTTMS works to identify the users consuming the most site resources, and reallocates a portion of the resources serving the data intensive users to other users engaged in less resource intensive activities. When RTTMS is activated on a resource constrained site, customers engaged in data intensive applications may experience reduced performance until the site becomes unconstrained or the user moves to a non-resource constrained site. Users of the resource-constrained site that are not engaged in data intensive actives should expect a better experience than they would have on the site if RTTMS not activated. Sprint's RTTMS is user, content, application, and device agnostic and is intended to provide an improved experience for the majority of users when resources are constrained.

12. Text: Describe the text capability that will be offered with your NPSBN, specify if it is separate from the public SMS/MMS service, the typical and maximum message delivery delay, and any particular features it provides for public safety users.

Sprint text capability is not separate from the Sprint public SMS/MMS service.

13. PTT: Describe the capabilities of your current push-to-talk (PTT) service including interface to existing LMR systems.

Sprint has been the leader in Sprint push-to-talk (PTT) services for over twenty years. Building on our experience, Sprint continues to deliver our innovation and leadership in PTT service; allowing individuals and groups to get more done quickly and easily with just the push of a button.

- **Sprint Direct Connect Plus** – Connect with another 1:1 push-to-talk user nationwide/on the Nationwide Sprint Network with the push-to-talk button
- **Large Group Calling** – Connect with up to 250 other users simultaneously anywhere on the Nationwide Sprint Network.
- **Call Alert** – send repeating call alerts or text messages to let recipients know you need to reach them

Built on cutting edge technology, Sprint Direct Connect Plus goes far and beyond traditional push-to-talk. Advanced features that deliver enhanced functionality include:

- **Simultaneous data and push-to-talk** – check received and sent email/texts;/instant messages; access the Internet for corporate networks and run data intensive applications, all while carrying on a put-to-talk conversation
- **Call alert with text** – send a message along with a call alert to any Sprint Direct Connect Plus-capable phone.
- **International push-to-talk service**—Connect instantly from the U.S. with international PTT users throughout Chile, Peru, Argentina and Brazil

Enhanced PTT features and expanded functionality:

- **Supervisor override** – gives supervisors ability to take over calls
- **Broadcast calling** – creates one-way calls to large groups of up to 500 members at once
- **PTT Wi-Fi Capability** – provides improved and cost- effective connectivity
- **QoS Monitoring** - to prioritize PTT traffic over regular data/internet traffic.
- **Tablet compatibility** – gives more device options to connect efficiently
- **Presence status** – allows users to indicate availability on devices
- **Improved LMR Land Mobile Radio interoperability** – extends the reach of dispatch
- **Talkgroup Scanning with priority** – allows users to monitor group call activity

14. MCPTT: Describe you plan and timetable for introducing Mission Critical PTT (MCPTT) services:

- **Overall plans and timetables**

Sprint is in the process evaluating the implementation of Mission Critical PTT. We expect to conclude the evaluation process by 2019.

- **Additional features to be provided with MCPTT**

Each of our button-enabled devices provides QoS while on the Sprint Network. This means the PTT calls are prioritized over the Sprint network. And with WPS these calls are prioritized further over 'ordinary' network calls. Additional features would follow the roadmap that Kodiak (the PTT platform owner) has and they are essentially rolling out all MC-PTT features in three phases which would be completed by late 2020.

- **Availability of direct peer-to-peer wireless device connectivity.**

Sprint Direct Connect Plus performs peer-to-peer connectivity, as well as, Groups.

- **Ability of MCPTT devices to continue to operate on a direct peer-to-peer basis if the cellular base station is disabled.**

Sprint Direct Connect Plus, depending on settings and devices, can operate on Wi-Fi and as a result, is not dependent on the cellular network.

- **Please describe what functions or capabilities would be lost in the event that the service cell site becomes inoperable.**

Presently peer to peer connectivity is not available without cellular service. Device manufacturer Sonim, is currently working on an accessory for two devices that is an off-network walkie talkie which would be supported on the two Sprint Sonim devices this year. If tower service is lost, the Sonim devices with this accessory will continue calls to the PTT channels. Details of the accessory functionality is unavailable at this time.

Service Level Agreements

15. Is there a specific, defined SLA for public safety customers? If so, please describe in detail.

At present, there are no specific defined SLA for public safety customers. Please see responses above for Voice Quality Performance Target/Guarantee and Broadband Data Performance Expectations/Guarantees.

Interoperability

16. Describe the level of interoperability between your solution and other cellular-based NPSBNs, FirstNet or other, for:

A. Voice Telephony (When Offered): Will public safety priority and QoS traffic classes be maintained for calls passing between different carriers' networks?

Sprint is in the process of evaluating interoperability between Sprint public network and other carrier's NPSBN.

B. Video Service: Will public safety priority and QoS traffic classes be maintained for video connections passing between different carriers' networks?

Sprint is in the process of evaluating interoperability between Sprint public network and other carrier's NPSBN.

C. Broadband Data: Describe how public safety priority and QoS traffic classes will be maintained for traffic passing between different carriers' networks?

Sprint is in the process of evaluating interoperability between Sprint public network and other carrier's NPSBN.

D. Text: Will NPSBN text services interoperate with users on other NPSBNs, and what other text services (e.g. SMS/MMS/RCS, Apple Messages, WhatsApp, etc.) can it exchange messages with.

Sprint is in the process of evaluating interoperability between Sprint public network and other carrier's NPSBN.

E. PTT: Describe interoperability between PTT users served on different carriers'

Sprint is in the process evaluating interoperability between PTT users served on different carriers.

F. MCPTT: Describe interoperability between MCPTT users served on different carriers' services, including stations that are:

- **Communicating through their cellular base station**
- **Communicating directly with one another (through Proximity Services)**
- **In the same broadcast group.**

Sprint is in the process evaluating interoperability between PTT users served on different carriers.

Network Management and Control

17. Does the vendor support a separate 'Portal' for public safety users?

Our complete suite of management tools and services are available to public safety users. At a high level, features include:

- **Lifecycle management for mobile devices**, including procurement, fulfillment, maintenance and replacement/retirement
- **Billing/expense management** via a simple, consolidated dashboard
- **Enhanced care** for dedicated, single-source service, support and proactive consultation
- **User-friendly web portal** for self-service inventory, usage and billing details
- **Detailed reporting/analysis** to optimize mobility investment across plans, services and carriers
- **Robust security services** for mobile devices and sensitive data
- **Policy tracking and enforcement** for your mobile enterprise assets

18. Does the vendor provide the ability for public safety customers to monitor network performance in real-time and a mechanism to communicate directly with network operations personnel during times of crisis?

The performance of Sprint's networks is monitored 24 hours a day, 7 days per week and 365 days a year by the Network Monitoring Centers. In addition, local switching offices staffed by trained technicians and management coordinate with these larger operations centers, to ensure that Sprint's networks are properly maintained. Customers can sign-up for alerts and notifications of network events.

19. Will government agencies have the ability to totally preempt public network voice/data/text traffic on shared elements in extreme circumstances to ensure public safety users maintain network availability at all times?

Yes, in the case of data traffic. All Public Safety voice traffic will be prioritized over commercial traffic. Total preemption of public network data traffic would be a rare occurrence. Preemption is used to allocate network resources to higher priority user's data flows. Lower priority user's data flows will be allocated fewer resources until higher priority users have sufficient resources.

Security, Reliability and Hardening Measures

20. Describe the security measures and standards employed for both traffic and control messages on both wired and wireless portions of the network.

Sprint Wireless Networks - The Sprint 3G and 4G-LTE wireless networks were designed with Confidentiality, Integrity, and Availability as cornerstones.

The Sprint 3G network used Code-Division Multiple Access (CDMA) to segregate user traffic. Each device has an Electronic Serial Number (ESN) that is matched to its Mobile Identification Number (MIN). At power-up, this pair of numbers is sent to the network for validation on the Home Location Register (HLR). Once authenticated, the device is allowed to make data connections. The network actively monitors all HLR registrations. When multiple instances of an ESN/MIN pair are detected, all devices using that pair are hot-lined and disabled. This technique, coupled with the difficulty of eavesdropping ESN and MIN combinations, reduces the opportunity for fraud by cloning a data-enabled Sprint device. For added resiliency and reliability our HLR database is 4x redundant, deployed in four geographically diverse data centers with complete redundancy (Chicago, Atlanta, Ft Worth, Nashville). This enables us to boast an HLR availability of 99.999%. Optional services, such as encrypted static web browsing and client initiated Virtual Private Network (VPN) are available to encrypt customer data traffic. In addition, devices are required to authenticate to the Subscriber Profile System (SPS) platform in order to utilize data services. Devices are required to authenticate with subscriber ID, Mobile Directory Number (MDN), and (International Mobile Subscriber Identify (IMSI). The SPS platform is geographically diverse with complete redundancy in Reston and two additional data center locations in Lenexa.

The Sprint 4G Long-Term Evolution (LTE) wireless network applies the most stringent authentication, ciphering, and encryption methodologies. 4G LTE technology is based on the Third Generation Partnership Project (3GPP) LTE standard, which defines the most comprehensive security architecture in the industry. The LTE Security architecture is covered in 3GPP Technical Specification 33.401. This architecture has introduced a key hierarchy to enhance both User and Data security. 4G LTE security features additional secure layers compared to previous wireless technologies such as the hierarchical key system. It also introduces forward security for Mobility (handoffs) and added protection when User Equipment moves from the 4G LTE network to the 3G Network. LTE security uses Non-Access Stratum (NAS) and Access Stratum (AS) functions to communicate with the various network elements. NAS messages carry out the security messages between User Equipment (UE) and the Mobility Management Entity (MME). NAS signaling protection between the UE and the MME are performed on the User Control plain and are protected by the NAS protocol. Integrity Algorithms are used to protect user information. By deploying the variety of security mechanisms described above, the Sprint 4G LTE Network offers built in secure communication, providing encryption and ciphering techniques and fraud protection mechanisms that lead the industry.

Sprint Wired Networks - Where appropriate, Sprint wireless traffic is backhauled through the Sprint Ethernet Wide Area Network (EWAN Network) wireline network. The EWAN also allows connectivity for wireline IP customers leveraging existing Sprint wireless infrastructure. The EWAN is based on a combination of Cisco Aggregation Services

Router (ASR) 9000 series and Juniper MX devices. Wireless traffic is routed on its own dedicated ports and separate routing tables. Virtual Routing and Forwarding (VRF) technology is used to segment customer traffic from control messages. The EWAN also uses advanced protocols, such as Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP) and Intermediate System to Intermediate System (IS-IS) to enhance network routing and performance.

Sprint Vendors/Suppliers - Regarding the security of our vendors, Sprint has a vetting process in place for vendors/suppliers that requires compliance with security laws and regulations governing protection of customer data. All vendors must be reviewed and approved before they are certified as eligible. This process also requires compliance with the Sprint Corporate Security standards for protection of Sprint information, equipment and personnel. If there are redlines to vetting requirements or language, Sprint Corporate Security is involved during the negotiation process to approve any changes to the security verbiage. In addition, key vendors are reviewed for financial risk each quarter. Any increases in risk are addressed by impacted business units.

From a security-risk perspective, vendor risk is handled in several ways. At the time of contract negotiations, lack of appropriate security verbiage in the contract is escalated via Supply Chain Management to the appropriate Sprint business unit. Also, when a known vendor security risk is identified in the product or service, Corporate Security documents this risk in a Security Risk Assessment which has a defined escalation process. Risk mitigation plans have also been developed for key vendors to address any significant impacts to Sprint resulting from outside vendor events. Periodic information security reviews are conducted on vendors with access to data and systems. Depending on the review level warranted, this is addressed several ways, through Corporate Audit Services, NSA audits, contract compliance reviews, and/or SOX audit processes.

21. Describe the overall network hardening for public safety services, and approach to meeting NPSTC public safety grade standards. Including but not limited to: battery backup, backup generator, redundant backhaul, etc.

As a Mobile Telecommunications Leader, the resiliency of Sprint's network is of paramount interest to our customers.

Network Incident Management Team

Network Services' implementation of the Incident Command System (ICS), stays true to the principles of ICS. This enables Sprint to leverage this best practice in wide-scale responses, using common terminology and standard organizational structures to communicate efficiently internally and with external customers such as Public Safety agencies as many of these agencies utilize ICS. Teams train on and deploy in standard ICS sections, branches, units and strike teams, and emphasize span of control, comprehensive resource management, and other ICS principles.

Network teams leverage Sprint tools such as hardened GPS-enabled phones, wireless modems, custom applications, M2M solutions and smart phones to aid in situation assessment, response and resource tracking. The teams also maintain a pool of Satellite phones as a contingency for use in restoration. Teams continue to create innovative response tools, such as the unique backhaul called Satellite Cell on Light Trucks (SatCOLTs) that enable restoration of service when a traditional backhaul is not available.

When the Network IMT receives notification of an actual or potential situation that requires activation (hurricane, earthquake, regional power outage, other event where business as usual would not resolve the situation), a virtual Emergency Operations Center (EOC) is established. This EOC performs an initial overall assessment, establishes monitoring bridge(s), coordinates between agencies impacted by the event, assigns tasks, gathers status information and performs executive notifications at prescribed times.

Cell Site Disaster Planning

Sprint's priority site restoration plan focuses resources and expedites recovery by making sure that existing infrastructure is operating properly under normal circumstances and by having a response plan for abnormal circumstances. To accomplish this, Sprint has implemented a detailed preventative maintenance program to insure all systems and redundant equipment are in proper working order. Sprint sites are equipped with battery backup. Some sites have fixed generators or fuel cells for additional back-up power. Sprint maintains a fleet of mobile generators deployable to Sprint service areas. Formal cell site classification designates all sites for criticality. Prioritization aids in properly allocating response personnel, generators and other resources.

Cellular Network Disaster Planning

Communications from Sprint cell sites are backhauled with various combinations of Ethernet, copper, fiber, and microwave systems. Most Sprint hub locations are placed on bi-directional fiber rings. These rings significantly reduce the chance of network failure due to third party fiber damage, equipment failures or other potential causes of service interruptions. Sprint's radio network provides significant overlapping coverage areas which often allow cell sites to fully or partially compensate for a neighboring cell site. In an effort to minimize service impact when a site is down, Sprint maintains a fleet of Cell Sites on Wheels (COWs) which are portable self-contained cell sites. COWs can be deployed to restore coverage from a damaged site or provide additional capacity in the immediate vicinity of an incident.

Switch Disaster Planning

Sprint has implemented a distributed architecture for interconnection redundancy utilizing dual fiber facilities at switch locations. Switch locations have battery backup as well as permanent generators. In addition, site recovery plans have been developed for all major switch locations, prioritizing available options for relocation, and ensuring agility when faced with disaster recovery issues. Most switches also have tap boxes that readily connect to the output of a portable generator in the event of primary generator issues.

Overall Network Performance Management Efforts

The performance of Sprint's networks is monitored 24 hours a day, 7 days per week and 365 days a year by the Network Monitoring Centers. In addition, local switching offices staffed by trained technicians and management coordinate with these larger operations centers, to ensure that Sprint's networks are properly maintained.

Network Restoration Prioritization

Sprint's Business Continuity Management Team works as a customer advocate when large network outages occur. The team works closely with network recovery teams to establish customer prioritization once the backbone, TSP (Telecommunications Service Priority) and Critical Life Circuits are re-established. Sprint has an established cell site classification and service restoration process.

Sprint's preparedness with hardware/systems at an alternate site is as follows:

If referring to a Sprint Data Center, the IT Incident Management Team identifies and prioritizes the recovery of IT applications process following the business strategy of "Serve, Sell, Bill, Report". This criterion allows IT to assess and align each application based on the business function and impact to print. An application alignment process is used to determine the priority of the application in the recovery timeline.

If referring to Network Assets, Sprint's Network Team compliments its assets with third parties when large network outages occur. Sprint has a very robust emergency response and disaster recovery plan which enables quick restoration of impacted services following a disaster. Sprint mitigates congestion risks through traffic management algorithms to handle the overload surges in traffic. Additionally, Sprint's well trained and exercised disaster recovery response teams proactively monitor congestion and performance of the wireless network and determine the appropriate course of action. This may include performing parameter changes, adding additional capacity to the network via radio installations to cell sites and/or by adding additional backhaul. Cell Site On-Wheels (COW) and Satellite On-Light-Trucks (SatCOLT) may also be used to replace and/or expand Sprint's foot print or add additional capacity to the network. Engineers use traffic history to provision network resources to support busy-hour traffic for cellular networks. Third parties are used to perform various functions such as reconnaissance, generator deployment/refueling, equipment repair, etc.

22. Does the vendor have the ability to augment coverage/capacity with deployable assets during events/disasters?

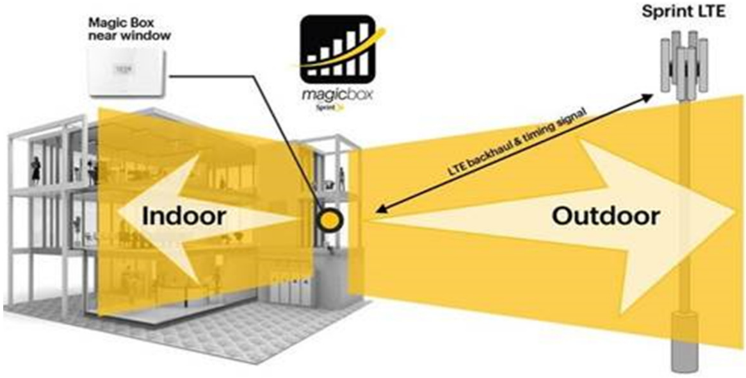
Yes, refer to response to # 8 above.

23. How would public safety or other government agency requests for those deployable assets be prioritized over public network services in an emergency or disaster situation?

Sprint's Emergency Response Team deployable systems are dedicated to supporting Government Operations. Government agencies can request support for deployable assets directly through Sprint's Emergency Response Hotline through our Toll Free Number at 888-639-0020 or GETS 254-295-2220. Additionally, requests can also be funneled through state ESF2 Communications Coordinators, Emergency Operations Center, FEMA Regional Response Coordinators, and the National Communications Coordinating Center (DHS NCC).

24. Does the vendor support local agencies purchasing their own cellular equipment to 'turn up' additional capacity when/where needed.

To provide seamless coverage and turn up additional capacity, Sprint has developed a plug 'n play small cell technology that improves performance of the 4G LTE network. This unique solution is known as the Sprint Magic Box. Sprint's Magic Box is a shoebox sized wireless femtocell relay device that is positioned on premise to increase signal strength in spectrum bands 41 and 25, and improve throughput of the Sprint 4G LTE Network. The Magic Box can enhance performance in areas up to 20,000 square feet, depending on environmental conditions.



Following are items included in the service:

- LTE+ small cell window booster
- High-speed data connectivity via Sprint 4G LTE network; **wireline web circuit not required**.
- Secure Wireless Ethernet bridge *(only included in qualified scenarios*)*

The equipment and monthly data service provided on premise is included. For service to become operational, the Sprint small cell repeater must be correctly placed and plugged into AC power. Below is an example of how the solution works within a commercial building and business.

30,000 sq. ft. Indoor Coverage
100 Meters Outdoor Coverage
LTE Plus
More spectrum. Better network.
Wireless Backhaul

- ✓ Flexible placement and operation
- ✓ Standard 110v outlet connection
- ✓ Draws only 35 watts of electricity
- ✓ Can discreetly deploy via placement inside a lighted window sign

Features and Benefits

- ♦ **Plug-n-play deployment** - No engineering, construction or specialized labor required
- ♦ **Boosts Sprint's LTE signal and throughput** - Delivers enhanced signal and faster speeds
- ♦ **Enhanced Coverage** - Depending on placement location it can provide enhanced network coverage typically up to 70-90% or more in domestic US retail locations

User Classification, Authorization and Onboarding

25. Detail classes of user priority defined and procedures required in applying for and initiating public safety priority service for a user as well as the mechanism for device provisioning and management in both day-to-day operations and during critical incidents.

Sprint ensures priority treatment and access to your data by adding Priority Service for Data on qualified Public Safety/First Responders wireless line of service. Sprint is targeting 2nd Quarter 2019 for Priority Service for Data.

Data Prioritization includes:

- Ability for qualified Public Safety/First Responder/Safety Officer users to get Access Prioritization on the Radio Access Network (RAN) over normal data users during heavy network utilization.
- Ability for Resource Prioritization so more RAN resources are assigned to qualified Public Safety/First Responder users during heavy network utilization.
- Ability for Higher transport prioritization (QoS) on the Core transport network.

Preemption

Sprint is looking to support Network Data Preemption with the capability targeted for availability 2nd Quarter 2019. However, given Sprint's unique spectrum position and network capacity there could be more effective alternatives.

26. Describe the process for a user to use his/her personal mobile device to access the public safety network services if required.

As an account administrator, you will be able to identify which user should receive Priority Service for Data treatment. These users will have the Priority Service for Data service available and receive prioritization during times of heavy network utilization. Sprint continues to review capabilities that will give account administrator's access to a portal that will give them the option to select individual users under their account and enable priority in real time fashion.

27. Confirm your ability to activate equipment and priority data/video services within 24 hours after request in the event of a State of Disaster/Emergency.

WPS is available only for authorized NS/EP users. The DHS/OEC has established five categories to identify critical NS/EP leadership functions and determine eligibility. Ultimately, DHS/OEC has approval for use of the service feature as well as defining to the carrier the approved use level. Participating entities can contact their local sales or care representative with requests to activate equipment within 24 hours upon a State of Disaster/Emergency. Additionally, entities can contact our Emergency Response Hotline 24x7x365 at (888) 639-0020 for after hours' assistance.

Homeland Security

Office of Emergency Communications

June 2016

HELPFUL TIPS FOR USERS OF WIRELESS PRIORITY SERVICE (WPS) AND GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE(GETS)

WPS Calling Instructions

For priority treatment from mobile phones:
- Requires phone subscription to WPS
- Enter *272 + Destination Number + Send (example: *272 + 202-555-1212 + Send)
- Optional *272 + 1 - 202-555-1212 + Send

GETS Calling Instructions

For priority treatment from any phone:
1. Dial 1-710-627-4387
2. At the tone, enter your PIN
3. When prompted, enter your destination number (area code + number, or international number). Do not enter a 1 before the destination area code.

MAKE REGULAR GETS AND WPS PRACTICE/TEST CALLS

Make GETS and WPS practice/test calls from phones you might use in an emergency. This helps ensure priority calling is possible from your phones, and helps you maintain proficiency with GETS and WPS. Use the Familiarization Line, 703-818-3924, or a phone number you may dial in an emergency, as the destination number.

PREPROGRAM *272 FOR KEY NUMBERS IN YOUR PHONE'S CONTACT LIST

In an emergency, it takes time (and a good memory) to look up a phone number and then manually dial *272 + the number. Instead, add *272 to key numbers in your mobile phone's contact list so you can call them using WPS with the push of a single button. For example:

John Smith work: 202-555-1212   John Smith work 2: *272 + 202-555-1212

GETS/WPS DIALER APPLICATION FOR SMARTPHONES

A GETS/WPS Dialer Application, or "app," is available for Android smartphones. The app provides a simplified way for users to make GETS and WPS calls to numbers stored in the smartphone's contact list and Call Log, as well as to numbers entered via keypad dialing. The GETS/WPS Dialer App for Android and Blackberry smartphones is available for download at **http://gets-wps.csgov.com/apps**.

GETS OPERATOR SUPPORT

GETS callers desiring operator support should wait 6-8 seconds without entering the PIN and the call will time out to Sprint or Verizon GETS operator support. Please follow the operator's guidance so that your call is processed correctly. AT&T does not provide GETS operator support. Operator Support will also be available on the Sprint Internet Protocol (IP) Network by the fourth quarter of 2016.

DO NOT USE GETS OR WPS TO DIAL 911

GETS does not allow calls to 911, and WPS carriers do not support WPS calls to 911.

TEST WPS AFTER CHANGES

Make a WPS test call after a phone upgrade or account change. Report any service problems to your GETS/WPS Point of Contact (POC) or 24 Hour User Assistance at 1-800-818-4387 or 703-818-4387.

KEEP YOUR GETS CARD WITH YOU

Keep your GETS card in your wallet, purse, or somewhere easily accessible so you will have it when you need it. Note that WPS dialing instructions appear on the back of the card. If you cannot find your card, please contact your GETS/WPS POC for a replacement.

YOU MAY EXPERIENCE SILENCE AFTER ENTERING YOUR DESTINATION NUMBER

During network congestion, GETS and WPS may place your call in a queue until a circuit becomes available. While waiting, you may hear silence or intermittent tones. Stay on the line until your call completes. Depending on the circumstances, this could take 30 seconds or longer.

USING WPS + GETS TOGETHER MAY HELP IN CERTAIN CIRCUMSTANCES

In some cases, using WPS and GETS together can improve the probability of call completion. You can preprogram your WPS subscribed phone to dial *272 + 710-627-4387 + [pause] + GETS PIN so that you only need to enter the final destination number.

REPORT CALLING TROUBLE

If you encounter a problem while using GETS or WPS, report it to 24 Hour User Assistance at 1-800-818-4387 or 703-818-4387. These numbers are also located on the back of your GETS card.

THERE ARE ALTERNATE ACCESS NUMBERS FOR MAKING A GETS CALL

The back of your GETS card lists alternate dialing sequences in case the universal access number, 1-710-627-4387, does not work:
1-888-288-4387 (AT&T)
1-877-646-4387 (AT&T IP Network)
1010 + 288 + 1-710-627-4387 (AT&T) - for use from landline phones only
1-800-257-8373 (Sprint)
1-855-333-4387 (Sprint IP Network)
1010 + 333 + 1-710-627-4387 (Sprint) - for use from landline phones only
1-800-900-4387 (Verizon)
1-855-400-4387 (Verizon IP Network)
1010 + 222 + 1-710-627-4387 (Verizon) - for use from landline phones only

YOU MUST HAVE ACCESS TO THE PHONE NETWORK

To make a GETS call from a landline device, you must have a dial tone. To make a GETS or WPS call from a mobile phone, you must have a cellular signal. If you have no signal (no bars), try calling from another location. If the network infrastructure is unavailable (for example, due to power failure or physical damage) GETS and WPS will not work.

CALLING TOLL-FREE DESTINATION NUMBERS USING GETS AND WPS

Use the Sprint IP Network GETS access number, 1-855-333-4387, to place GETS calls to toll-free destination numbers. Other GETS access numbers currently do not allow calls to toll-free destination numbers. As a contingency, find out in advance the local translations of the 800, 888, 877, 866, 855, or 844 numbers your organization uses in emergencies and distribute this information to your GETS users. WPS allows priority calls to toll-free destination numbers.

FOR LANDLINE CALLS, WAIT FOR A DIAL TONE

During times of congestion you may have to wait for a dial tone after picking up the receiver. Hanging up and picking up the receiver again will only delay assignment of a dial tone.

GETS CALLS CAN BE MADE FROM ANY PHONE

GETS is available nationwide and can also be accessed from international locations. GETS can also be accessed through the Defense Switched Network, Networx, the Diplomatic Telecommunications Service, and the FEMA Switched Network. GETS calls may also be placed from satellite phones, though they will not receive priority treatment until they are routed to the landline network.

CHECK YOUR PRIVATE BRANCH EXCHANGE (PBX)

If you are calling from an office building served by a PBX that has stopped working, try using a device connected directly to the phone company's central office. Often, fax machines, modems, payphones, secure telephones, and teletypewriters use these connections. Emergency managers should identify the devices in their facilities that are connected directly to the central office and record the devices' locations and phone numbers in their emergency planning documents.

WPS CALLS FROM VOICE OVER LONG TERM EVOLUTION (VOLTE)-ENABLED MOBILE PHONES

Cellular carriers are transitioning their networks to the next generation of cellular network technology, referred to as Long Term Evolution (LTE) or 4th Generation (4G). The carriers have been offering data on LTE, but now are introducing VoLTE. Each carrier will phase in VoLTE over different timeframes. Since WPS capabilities currently operate on 2G/3G networks, the transition to VoLTE may have an impact on WPS subscribers. Before subscribing to VoLTE service, WPS subscribers should check with their service provider to determine the impact to WPS capabilities. Further information is available in the June 2015 GETS/WPS NewsNotes, and is available to POCs on the GETS-WPS Information Delivery Service at **https://gets-wps.csgov.com**.

BE AWARE OF GETS AND WPS LIMITATIONS ON WIFI NETWORKS

Many cellular carriers incorporate WiFi connectivity into mobile phones in order to increase the coverage and capacity of their networks. WiFi connectivity is utilized for both data and voice (i.e., Voice over WiFi) communications. Currently, there is no priority on the WiFi network segment of GETS and WPS calls. If your GETS or WPS calls on a WiFi network do not go through, try completing your call on your mobile service provider network by disabling Wi-Fi on the mobile phone or physically moving beyond the range of the Wi-Fi network.

BE AWARE OF WPS LIMITATIONS ON SMALL CELL SITES (PICOCELLS AND FEMTOCELLS)

WPS calls made from within the range of small cell sites (e.g., inside buildings) may be rejected. Instead, try making a GETS call, or move outside and try to make the WPS call.

DHS PRIORITY TELECOMMUNICATIONS CONTACT INFORMATION

Service Center: 1-866-627-2255, 1-703-676-2255
User Assistance: 1-800-818-4387, 1-703-818-4387

Website: **www.dhs.gov/gets, www.dhs.gov/wps**

Who Should Enroll?

ORGANIZATIONS	INDIVIDUALS
• Cities/counties/states/districts/tribes/territories • Office of Emergency Management • Police/Sheriff/Fire/Emergency Medical Services • Water, power and telecommunications • Public works • Irrigation districts/flood control • Public health • Financial institutions • Hospitals/medical services • Transit agencies • Ports/airports • Transportation • Search and rescue • School districts and colleges • Red Cross/volunteer agencies • Critical infrastructure suppliers • Other agencies included in emergency management plans	• Executive leadership (Governor, Mayor, council members, city manager, supervisors, and staff) • Chief Financial Officer • Media relations • Office of Emergency Management and staff • Police/Fire Chiefs and staff • Police/Fire field command • Department heads and key staff • Subject matter experts/trained specialists • Individuals with an NS/EP role • Continuity Planning/Continuity of Operations staff
FACILITIES/LOCATIONS	
• Primary and backup Emergency Operations Centers • Public safety answering points (911 center) • Computer/IT center	• Police/Fire dispatch • City/county yards • Remote offices/stations • Power/pump stations • Shelters • Command vehicles

Enrollment Process

The first step in the enrollment process is to establish a point of contact (POC) for your organization. Many organizations already have established POCs who facilitate the enrollment process. To determine your POC and enroll in the priority services programs, please contact the DHS Priority Telecommunications Service Center at (866) 627-2255, or visit one of the following websites: www.dhs.gov/gets, www.dhs.gov/wps, or www.dhs.gov/tsp.

About the Office of Emergency Communications

Housed in DHS's National Protection and Programs Directorate's Office of Cybersecurity and Communications, OEC supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. The office leads the Nation's operable and interoperable public safety and NS/EP communications efforts. Offering training, coordination, tools, and guidance, OEC coordinates with federal, state, local, tribal and territorial governments, and industry partners to ensure that communications are available at all times. For more information about OEC, please visit www.dhs.gov/oec.

Department of Homeland Security
Office of Emergency Communications

Web: www.dhs.gov/oec

Priority Telecommunications Services

Homeland Security

The Department of Homeland Security (DHS) Office of Emergency Communications (OEC) offers a suite of Priority Telecommunications Services designed to support national security and public safety communications availability for government officials, emergency responders, and critical infrastructure owners and operators.

Government Emergency Telecommunications Service (GETS)

GETS is designed to provide priority landline and some cellular calling capabilities when communications networks are congested.

- GETS provides authorized personnel with priority for local and long distance calls.
- GETS calls can be made from any phone; no special equipment is needed.
- There is no charge to enroll in GETS or to make calls to the familiarization line.
- GETS has historically provided more than a 95 percent call completion rate during emergency response incidents.
- GETS calls made on cell phones receive some priority access on WPS cellular networks, even if the individuals making and receiving the calls do not have WPS.

> *"After the National Capital Region experienced an earthquake, our phone lines were jammed. But thanks to GETS, I was able to get connected."*
>
> *- Adam Thiel, former Alexandria (VA) Fire Chief*

Wireless Priority Service (WPS)

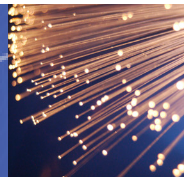
WPS is designed to provide priority cellular calling capabilities when communications networks are congested.

- Callers dial *272 from an enrolled cellular phone followed by the destination number to make a WPS call.
- The WPS service is added on a per-cell phone basis; calls must be placed on a subscribed phone to initiate priority calling.
- WPS subscribers are responsible for initial enrollment, monthly subscription, and per-call charges. These charges vary by cellular carrier.
- WPS has historically provided more than a 93 percent call completion rate.

> *"My cellular calls would not go through unless I used WPS. My calls went through, that's the bottom line. It worked really well for us."*
>
> *- Willie Collins, Emergency Support Function #2 Communications Planner at the 2016 Louisiana flooding response and recovery operations.*

While both GETS and WPS provide priority calling, they do not disrupt calls currently in process or prevent the general public's use of the telecommunications networks.

Telecommunications Service Priority (TSP)



The TSP program provides national security and public safety organizations with a way to receive priority installation and repair of critical data and voice communications circuits. A Federal Communications Commission mandate ensures that service vendors prioritize requests for new or repaired circuits for organizations enrolled in TSP.

- Organizations can request TSP priority installation and repair outside of an emergency when normal vendor service times do not meet the organization's needs.
- Enrolled organizations are subject to minimal TSP enrollment and monthly subscription charges from their service providers. These charges are established by the state Public Utility Commission and vary by carrier, location of the circuits, and other factors.
- Telecommunications vendors are legally obligated to restore TSP-coded circuits before circuits under service level agreements (SLA), even if this causes noncompliance with an SLA.

> *"The State of Arizona 9-1-1 Office has been using the TSP program since 2006 on our network for 9-1-1 call-taking services. We have approximately 1,250 circuits that have the added feature of priority restoration with the provider in case of a disaster involving large areas of population. It is important to Arizona that all available resources are considered when it comes to the health and well-being of our citizens."*
>
> *- Barbara A. Jaeger, Arizona State 9-1-1 Administrator*

Eligibility Criteria

The national security and emergency preparedness (NS/EP) community spans the federal, state, local, tribal and territorial governments; public safety and emergency responders; industry partners who are responsible for maintaining the Nation's critical infrastructure; and other authorized users. Organizations that rely on telecommunications on a daily basis to protect public health, maintain law and order, ensure public safety, and/or provide financial or utility service should enroll in these vital priority services. Typical GETS, WPS, and TSP users are responsible for the command and control functions critical to management of, and response to, national security and civil emergencies.

NASPO ValuePoint

NASPO ValuePoint Wireless Data, Voice and Accessories
Product Add Request

DATE: _________

ATTN: Chris Jennings
NASPO ValuePoint Contract Administrator

RE: NASPO ValuePoint Master Service Agreement # (the “Contract”) with _________(“Contractor”)

Dear Mr. Jennings:

Action Requested:

Contractor requests to add the product(s) and/or service(s) referenced in this document (collectively, the “Products”) to the Contract.

Action Log: _____Verify Log is attached

PRODUCTS:

PRODUCT OVERVIEW:

Provide a summary of the product you are requesting to add. Attach any product brief to this document.

Describe how the product falls with the Scope of the Master Agreement:

____
____
____
____

NEW PRODUCT TERMS AND CONDITIONS. Attach any Terms and Conditions that apply to this product (such as ULA, Policy, Product Terms and Conditions). Any and all Products offered and furnished shall comply fully with all applicable Federal and State laws and regulations. Any third-party product provider must agree to the Master Agreement Terms and Conditions.

NASPO ValuePoint

NASPO ValuePoint Wireless Data, Voice and Accessories
Product Add Request

BILLING

Any Product added to the NASPO ValuePoint Master Agreement must be billed by the Master Agreement Contractor and not by any third party.

COST:

Include a cost matrix to include NASPO ValuePoint contract pricing.

NASPO ValuePoint

NASPO ValuePoint Wireless Data, Voice and Accessories
Product Add Request

APPROVAL:

Upon signature, NASPO ValuePoint approves the addition of the product(s) and/or service(s) referenced herein to the Contract.

Upon signature, Contractor assures that all product(s) and/or service(s) referenced herein meet the terms and conditions of the Contract and understands that NASPO ValuePoint reserves the right to audit Contractor for compliance in accordance with the terms and conditions of the Contract. NASPO ValuePoint also reserves the right (a) to request additional information with respect to the product(s) and/or service(s) throughout the life of the Contract if in the best interest of NASPO ValuePoint.

Contract Vendor:

BY: ______________________________

NAME: ______________________________

TITLE: ______________________________

DATE: ______________________________

NASPO ValuePoint

BY: ______________________________

NAME: ______________________________

TITLE: ______________________________

DATE: ______________________________

NASPO ValuePoint Wireless Data, Voice and Accessories
Product Add Request

ACTION LOG

Submit updated Action Log with each Request. Log must provide history of previous requests.

CONTRACT VENDOR:___________________________

Contact Name and Email (for questions):___________________________________

DATE:___________________

DATE SUBMITTED	ACTION REQUESTED:	DATE APPROVED

MA262-1
Attachment S
Technology Disclosures

CSA Consensus Assessments Initiative Questionnaire

May 2017

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

Introduction

The Cloud Security Alliance (CSA) is a “not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.” For more information, see https://cloudsecurityalliance.org/about/.

A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

CSA Consensus Assessments Initiative Questionnaire

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Application & Interface Security *Application Security*	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. AWS has procedures in place to manage new development of resources. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	AWS Customers retain responsibility to ensure their usage of AWS is in compliance with applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/compliance) and providing certifications, reports and other relevant documentation directly to AWS Customers.
	AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	
Application & Interface Security *Data Integrity*	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	AWS data integrity controls as described in AWS SOC reports illustrates the data integrity controls maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 14 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	AWS Data Security Architecture was designed to incorporate industry leading practices. Refer to AWS Certifications, reports and whitepapers for additional details on the various leading practices that AWS adheres to (available at http://aws.amazon.com/compliance).
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third-party attestations and provides certain certifications, reports and other relevant documentation directly to AWS Customers.
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. The AWS ISO 27001 certification can be downloaded here. The AWS SOC 3 report can be downloaded here. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external audits and risk assessments. AWS engages with external certifying bodies and independent
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best	

Control Group	CID	Consensus Assessment Questions	AWS Response
		practices and guidance?	auditors to review and test the AWS overall control environment.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security
	AAC-03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 and Glacier services are designed to drive the likelihood of data loss to near zero percent and

Control Group	CID	Consensus Assessment Questions	AWS Response
			the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website.
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
	AAC-03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	AWS monitors relevant legal and regulatory requirements. Refer to ISO 27001 standard Annex 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Cloud Security whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	AWS Customers designate in which physical region their data and servers will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. AWS SOC reports provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing.
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security/. Refer to ISO 27001 Appendix A Domain 12.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR-07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	BCR-07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Cloud Security Whitepaper - available at http://aws.amazon.com/security.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	AWS CloudWatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	
Business Continuity Management & Operational Resilience *Policy*	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance.
Business Continuity Management	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	AWS provide customers with the ability to delete their data. However, AWS Customers retain control and ownership of their data so it is the customer's responsibility to manage data

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
& Operational Resilience *Retention Policy*	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	retention to their own requirements. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. For additional information refer to https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	AWS backup and redundancy mechanisms have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 12 and the AWS SOC 2 report for additional information on AWS backup and redundancy mechanisms.
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Whether a customer is new to AWS or an advanced user, useful information about the services, ranging from introductions to advanced features, can be found on the AWS Documentation section of our website at https://aws.amazon.com/documentation/.
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	
Change Control & Configuration *Management* *Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	AWS maintains an ISO 9001 certification. This is an independent validation of AWS quality system and determined that AWS activities comply with ISO 9001 requirements. AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to aws.amazon.com/security/security-bulletins/. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS system development lifecycle (SDLC) incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. In addition, refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	AWS' program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management *Production Changes*	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?	AWS SOC reports provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 12 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user-friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console has also supports tagging.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	AWS Customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public	All of the AWS APIs are available via SSH-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
		networks (e.g., the Internet)?	control encryption keys (refer to https://aws.amazon.com/kms/). Customers may also use third-party encryption technologies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	AWS Customers retain control and ownership of their own data. Refer to the AWS Customer Agreement for additional information.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	
Datacenter Security *Asset Management*	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Datacenter Security *Controlled Access Points*	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Equipment Identification*	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Offsite Authorization*	DCS-04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	AWS Customers can designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Datacenter Security *Offsite equipment*	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Datacenter Security *Policy*	DCS-06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 and SOC 2 reports provides further information.
Datacenter Security *Secure Area Authorization*	DCS-07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	AWS Customers designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
Datacenter Security *Unauthorized Persons Entry*	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security *User Access*	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Encryption & Key Management *Entitlement*	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key Management *Key Generation*	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	
	EKM-02.3	Do you maintain key management procedures?	
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key Management *Encryption*	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	
	EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	
Encryption & Key Management	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Storage and Access		and standard algorithms?	Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	
Governance and Risk Management *Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standards, Annex A, domain 14 and 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Governance and Risk Management *Risk Assessments*	GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS Customers. Continuous Monitoring of logical controls can be executed by customers on their own systems.
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/.
Governance and Risk Management *Management Oversight*	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AWS provides our customers with our ISO 27001 certification. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how AWS internal processes follow the ISO standard. Certification means a third party accredited independent auditor has

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	performed an assessment of our processes and controls and confirms they are operating in alignment with the ISO 27001 certification standard. For additional information refer to the AWS Compliance ISO 27001 FAQ website: http://aws.amazon.com/compliance/iso-27001-faqs/.
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	AWS has established information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance. Information about the AWS Compliance programs is published publicly on our website at http://aws.amazon.com/compliance/.
Governance and Risk Management *Policy*	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management *Policy Enforcement*	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	AWS provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	(e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
Governance and Risk Management *Policy Reviews*	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Our AWS Cloud Security Whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security and http://aws.amazon.com/compliance, are updated on a regular basis to reflect updates to the AWS policies.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	The AWS SOC reports provide details related to privacy and security policy review.
Governance and Risk Management *Assessments*	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at aws.amazon.com/security) for additional details on AWS Risk Management Framework.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	
Governance and Risk Management *Program*	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk. AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. AWS Risk Management program is reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	
Human Resources *Asset Returns*	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	AWS Customers retain the responsibility to monitor their own environment for privacy breaches. The AWS SOC reports provides an overview of the controls in place to monitor AWS managed environment.
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	
Human Resources *Background Screening*	HRS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. The AWS SOC reports provides additional details regarding the controls in place for background verification.

Control Group	CID	Consensus Assessment Questions	AWS Response
		subject to background verification?	
Human Resources *Employment Agreements*	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	In alignment with ISO 27001 standard, all AWS employees complete periodic role based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details. All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	
Human Resources *Employment Termination*	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. AWS SOC reports provide additional details.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Human Resources *Portable / Mobile Devices*	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Human Resources *Nondisclosure Agreements*	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Human Resources *Roles / Responsibilities*	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	The AWS Cloud Security Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security and http://aws.amazon.com/compliance.
Human Resources *Acceptable Use*	HRS-08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content. Refer to the ISO 27001 standard and 27018 code of practice for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 and ISO 27018.
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	
Human Resources *Training / Awareness*	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
		regard to security and data integrity?	
Human Resources *User Responsibility*	HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 7 and 8. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition the AWS Cloud Security Whitepaper provides further details - available at http://aws.amazon.com/security.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources *Workspace*	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8 and 9. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS-11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	related events in accordance with requirements. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.
Identity & Access Management *Audit Tools Access*	IAM-01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IAM-01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP compliance.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Identity & Access Management *User Access Policy*	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM-02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored per the AWS access policy. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
Identity & Access Management *Policies and Procedures*	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	
Identity & Access Management *Segregation of Duties*	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Customers retain the ability to manage segregations of duties of their AWS resources. Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	
Identity & Access Management *Third Party Access*	IAM-07.1	Do you provide multi-failure disaster recovery capability?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC reports provides further details. ISO 27001 standard Annex A, domain 15 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM-07.3	Do you have more than one provider for each service you depend on?	
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provided a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Identity & Access Management *User Access Restriction / Authorization*	IAM-08.1	Do you document how you grant and approve access to tenant data?	AWS Customers retain control and ownership of their data. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management *User Access Authorization*	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.
	IAM-09.2	Do you provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.

Control Group	CID	Consensus Assessment Questions	AWS Response
Identity & Access Management *User Access Reviews*	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports. Refer to ISO 27001 standards, Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	
	IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	
Identity & Access Management *User Access Revocation*	IAM-11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Access is automatically revoked when an employee’s record is terminated in Amazon’s Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Identity & Access Management *User ID Credentials*	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa. AWS Identity and Access Management (IAM) supports identity federation for delegated access to the AWS Management Console or AWS APIs. With identity federation, external identities (federated users) are granted secure access to resources in your AWS account without having to create IAM users. These external identities can come from your corporate identity provider (such as Microsoft Active Directory or from the AWS Directory Service) or from a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google or any OpenID Connect (OIDC) compatible provider.
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	
	IAM-12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	
	IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM-12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/. AWS SOC reports provides details on the specific control activities executed by AWS.
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	
	IAM-12.10	Do you support the ability to force password changes upon first logon?	
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	
Identity & Access Management *Utility Programs Access*	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides details on the specific control activities executed by AWS. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM-13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	
	IAM-13.3	Are attacks that target the virtual infrastructure	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
		prevented with technical controls?	
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	AWS Incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides additional details on controls in place to restrict system access. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	
	IVS-01.4	Are audit logs centrally stored and retained?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
			are quickly and reliably communicated to operations personnel. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and	Details regarding AWS Service Limits and how to request an increase for specific services is available on the AWS website at http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html.

Control Group	CID	Consensus Assessment Questions	AWS Response
		under what circumstances/scenarios?	AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
	IVS-04.3	Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of

Control Group	CID	Consensus Assessment Questions	AWS Response
			AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website - http://aws.amazon.com/documentation/.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	
	IVS-06.4	Are all firewall access control lists documented with business justification?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP^{sm}. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Interoperability & Portability *APIs*	IPY-01	Do you publish a list of all APIs available in the service and indicate which are	Details regarding AWS APIs can be found on the AWS website at https://aws.amazon.com/documentation/.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
		standard and which are customized?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Interoperability & Portability *Data Request*	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	
Interoperability & Portability *Policy & Legal*	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	AWS allows customers to move data as needed on and off AWS storage. Refer to http://aws.amazon.com/choosing-a-cloud-platform for more information on Storage options.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Interoperability & Portability *Virtualization*	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	
Mobile Security *Anti-Malware*	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional information.
Mobile Security *Application Stores*	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	AWS has established an information security framework and policies and has effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Mobile Security *Approved Applications*	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	
Mobile Security *Approved Software for BYOD*	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
		approved for use on BYOD devices?	
Mobile Security *Awareness and Training*	MOS-05	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	
Mobile Security *Cloud Based Services*	MOS-06	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	
Mobile Security *Compatibility*	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security *Device Eligibility*	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security *Device Inventory*	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Mobile Security *Device Management*	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security *Encryption*	MOS-11	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	
Mobile Security *Jailbreaking and Rooting*	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Legal*	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS-13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Lockout Screen*	MOS-14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security *Operating Systems*	MOS-15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	
Mobile Security *Passwords*	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security *Policy*	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security *Remote Wipe*	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	
Mobile Security *Security Patches*	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	
Mobile Security *Users*	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed	

Control Group	CID	Consensus Assessment Questions	AWS Response
		access via a BYOD-enabled device?	
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The AWS SOC reports provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	
	SEF-02.4	Have you tested your security incident response plans in the last year?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of AWS services. Refer to AWS SOC report for specific details in relation to Data Integrity and Access Management (including least privilege access)
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC reports provides details on the specific control activities executed by AWS. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 15 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information. AWS does not generally outsource development of AWS services to subcontractors.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
	STA-05.3	Does legal counsel review all third-party agreements?	
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	
	STA-05.5	Do you provide the client with a list and copies of all sub processing agreements and keep this updated?	
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	AWS maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. AWS' third party management processes are reviewed by independent auditors as part of AWS ongoing compliance with SOC and ISO 27001.

Control Group	CID	Consensus Assessment Questions	AWS Response
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	

Control Group	**CID**	**Consensus Assessment Questions**	**AWS Response**
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC reports provides additional details on the specific control activities executed by AWS.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to AWS Cloud Security Whitepaper for further information - available at
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed	

Control Group	CID	Consensus Assessment Questions	AWS Response
		by industry best practices?	http://aws.amazon.com/security. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management *Mobile Code*	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	AWS allows customers to manage client and mobile applications to their own requirements.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	

Further Reading

For additional information, see the following sources:

- AWS Risk and Compliance Overview
- AWS Certifications, Programs, Reports, and Third-Party Attestations
- AWS Answers to Key Compliance Questions

Document Revisions

Date	Description
January 2017	Migrated to new template.
January 2016	First publication

Cloud Security Alliance (CSA) STAR Self-Assessment

Azure | Dynamics 365 | Office 365

The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud.

In 2010, the CSA published a suite of tools to assess cloud IT operations: the CSA Governance, Risk Management, and Compliance (GRC) Stack. It was designed to help cloud customers assess how cloud service providers (CSPs) follow industry best practices and standards, and comply with regulations.

In 2013, the CSA and the British Standards Institution launched the Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry in which CSPs can publish their CSA-related assessments.

CSA STAR is based on two key components of the CSA GRC Stack:

- Cloud Controls Matrix (CCM): a controls framework covering fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a CSP.
- The Consensus Assessments Initiative Questionnaire (CAIQ): a set of more than 140 questions based on the CCM that a customer or cloud auditor may want to ask of CSPs to assess their compliance with CSA best practices.

STAR provides three levels of assurance; CSA STAR Self-Assessment is the introductory offering at Level 1, which is free and open to all CSPs. Going further up the assurance stack, Level 2 of the STAR program involves third-party assessment-based certifications, and Level 3 involves certifications based on continuous monitoring.

As part of the STAR Self-Assessment, CSPs can submit two different types of documents to indicate their compliance with CSA best practices: a completed CAIQ, or a report documenting compliance with CCM. For the CSA STAR Self-Assessment, Microsoft publishes both a CAIQ and a CCM-based report for Microsoft Azure, and CCM-based reports for Microsoft Dynamics 365 and Microsoft Office 365.

Helpful information

Cloud Security Alliance
cloudsecurityalliance.org

CSA Security, Trust & Assurance Registry (STAR)
cloudsecurityalliance.org/star

About CSA STAR Self-Assessment
aka.ms/csa-star-self-assess

Cloud Controls Matrix (CCM)
aka.ms/CSACCM

Consensus Assessments Initiative Questionnaire (CAIQ)
aka.ms/CSA-CAIQ

Azure Responses to the CSA CAIQ v3.0.1
aka.ms/csacaiqresponses

Microsoft CSA STAR Self-Assessments

- **Azure** (aka.ms/Azure_STAR)
- **Dynamics 365** (aka.ms/DynamicsCRM_Online_STAR)
- **Office 365** (aka.ms/Office365_STAR)

Microsoft Common Controls Hub Compliance Framework
aka.ms/MCCH

Microsoft Trust Center
www.microsoft.com/trustcenter

Frequently asked questions

Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks such as ISO 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. For the most current list, visit the Cloud Security Alliance website.

Why is the CSA STAR Self-Assessment important?

It enables CSPs to document compliance with CSA published best practices in a transparent manner. Self-assessment reports are publicly available, thereby helping cloud customers gain visibility into the security practices of CSPs, as well as compare various CSPs using the same baseline.

Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- **Level 1: CSA STAR Self-Assessment: Azure, Microsoft Dynamics 365, and Microsoft Office 365**. The Self-Assessment is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.

- **Level 2: CSA STAR Certification: Azure, Intune, and Microsoft Power BI** (aka.ms/CSA-STAR-Cert-background). STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.

- **Level 2: CSA STAR Attestation: Azure and Intune** (aka.ms/CSA-STAR-Atttest-background). CSA and the AICPA have collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. STAR Attestation is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

CSA cloud security alliance℠

January 2017

Microsoft Azure Responses to Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1

http://www.microsoft.com/trust

NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.

Version 1, Published March 2016

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Table of Contents

1 Introduction

The Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 provides a comprehensive set of questions that customers can use to evaluate the depth / breadth of cloud vendors' security, privacy, and compliance processes. The Microsoft Azure team has compiled detailed responses to the ~300 items in the assessment, laid out in the following sections according to their respective domains.

If you're contemplating a move to the public cloud, or are already in the midst of your migration, this document will be a valuable resource for understanding how Azure meets and exceeds the requirements set forth by the CSA. Below you will find information culled from Azure engineering, operations, and policies. In most cases, the responses are specific to Azure, but are identified when broader Microsoft policies apply.

We recommend also reviewing Azure's response to the CSA Cloud Control Matrix (CCM), which is available on the Microsoft Trust Center at http://www.microsoft.com/trust. This document is aligned 1:1 with the CAIQ, and similarly aligns with multiple international standards and compliance frameworks (for more information, see https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/) such as ISO 27001, PCI, and SOC. Microsoft audits against dozens of standards, and additional details can be obtained through the audit reports available from the Service Trust Portal at https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx).

Microsoft Azure Responses to CSA CAIQ v3.0.1

Application and Interface Security: Controls AIS-01 through AIS-04

Control ID in CCM[1]	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
AIS-01.1: Application & Interface Security - Application Security	*Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?*	Y			The Microsoft Azure trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures. Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state. Azure validates services using third-party penetration testing based upon the OWASP (Open Web Application Security Project) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to Microsoft security practices.
AIS-01.2: Application & Interface Security - Application Security	*Do you use an automated source code analysis tool to detect security defects in code prior to production?*	Y			Source code builds are scanned for malware prior to release to production. The Microsoft Anti-Malware Client and Service is installed by default and available for customers to enable in all Azure Cloud Services. The Microsoft Anti-Malware Client and Service is available as an optional security extension in the Virtual Machines platform.
AIS-01.3: Application & Interface Security - Application Security	*Do you use manual source-code analysis to detect security defects in code prior to production?*		N		A Final Security Review (FSR) is performed for software releases prior to production deployment by a designated Security Advisor outside of the Microsoft Azure development team. Web applications are scanned with the PortSwigger Burp Suite scanning solution.

[1] CCM content in columns 1 and 2 is © 2015 Cloud Security Alliance, used with permission.

AIS-01.4: Application & Interface Security - Application Security	*Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?*	Y			Services provided by third-party vendors are monitored against agreed upon service levels by responsible parties in Microsoft Azure, as defined in the Statement of Work (SOW). Procedures for monitoring breaches to contractual obligations and handling issues with vendors are established and attested via industry-standard audit processes such as SOC 1 and 2.
AIS-01.5: Application & Interface Security - Application Security	*(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?*	Y			Procedures have been established and implemented to scan for vulnerabilities on hosts in the scope boundary. Vulnerability scanning is performed on server operating systems, databases, and network devices with the QualysGuard vulnerability scanning tool. The vulnerability scans are performed on a quarterly basis at minimum, but Azure security teams employ continuous monitoring processes to detect potential issues on an ongoing basis. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Red-Team / Blue-Team exercises (See AIS-01.1) are also routinely performed and results used to make security improvements.
AIS-02.1: Application & Interface Security - Customer Access Requirements	*Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?*	Y			Before using Azure Services, customers are required to review and agree with the acceptable use of data and the Microsoft Azure service, as well as security and privacy requirements, which are defined in the Microsoft Online Services Use Rights, Microsoft Online Subscription Agreement, Microsoft Azure Platform Privacy Statement and Technical Overview of the Security Features in Microsoft Azure Platform. Microsoft was the first major cloud service provider to make contractual privacy commitments (as well as to incorporate the best practices encompassed by ISO 27018) that help assure the privacy protections built into in-scope Azure services are strong. Among the commitments that Microsoft supports are: **EU Model Clauses** EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft is the first cloud provider to receive this recognition. **ISO 27018** Microsoft is the first major cloud provider to adopt the international code of practice for cloud privacy. ISO was developed to establish a uniform, international approach to protecting the privacy of personal data stored in the cloud. The

					British Standards Institution independently verified that Microsoft Azure is aligned with the guideline’s code of practice. ISO 27018 controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer’s express consent.
AIS-02.2: Application & Interface Security - Customer Access Requirements	*Are all requirements and trust levels for customers’ access defined and documented?*	Y			Customer access controls and trust levels are described on the Microsoft Azure Trust Center website at https://www.microsoft.com/en-us/TrustCenter/default.aspx.
AIS-03.1: Application & Interface Security - Data Integrity	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?*	Y			Microsoft Azure defines acceptable standards to ensure that data inputs to application systems are accurate and within the expected range of values. Where appropriate, data inputs should be sanitized or otherwise rendered safe before being inputted to an application system. Developers follow Microsoft's SDL methodology which includes requirements for data input and output validation checks. Additional information can be found here: http://www.microsoft.com/en-us/sdl/. Internal processing controls are implemented within the Microsoft Azure environment in order to limit the risks of processing errors. Internal processing controls exist in applications, as well as in the processing environment. Examples of internal processing controls include, but are not limited to, the use of hash totals, and checksums.
AIS-04.1: Application & Interface Security - Data Security / Integrity	*Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?*	Y			Microsoft maintains and regularly updates the Azure Information Security Management Policy and information security guidelines, standard operating procedures for data security, and contractual commitments to international data protection directives which apply across Azure services. In addition, Microsoft Azure software updates are reviewed for unauthorized changes through Security Development Lifecycle (SDL) change and release management processes. Automated mechanisms are used to perform periodic (at least every hour) integrity scans and detect system anomalies or unauthorized changes. Microsoft applies SDL to design, develop, and implement Microsoft Azure services. SDL helps to ensure that communication and collaboration services are highly secure, even at the foundation level, and align with other industry standards including FedRAMP, ISO, and NIST.

Audit Assurance and Compliance: Controls AAC-01 through AAC-03

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
AAC-01.1: Audit Assurance & Compliance - Audit Planning	*Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?*	Y			No, however, Microsoft Azure independent audit reports and certifications are shared with customers in the format native to the type of audit. These certifications and attestations accurately represent how we obtain and meet our security and compliance objectives and serve as a practical mechanism to validate our promises for customers. ISO 27001 certifications for Microsoft Azure and Microsoft Cloud Infrastructure and Operations (MCIO) can be found on the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective and existing customers. In addition to providing a high level of assurance that our controls are operating as expected, the compliance framework also results in several important certifications and attestations for Microsoft's cloud infrastructure, including ISO/IEC 27001:2013 certification, SSAE 16/ISAE 3402 SOC 1 Type 1 and Type 2 and AT Section 101 SOC 2 and 3 Type 1 and Type 2 attestations, as well as FedRAMP Certification and Accreditation.
AAC-02.1: Audit Assurance & Compliance - Independent Audits	*Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?*	Y			ISO 27001 certifications for Microsoft Azure and MCIO can be found on the website of our external ISO auditor, the BSI Group. Additional audit information is available under NDA upon request by prospective and existing customers through their Microsoft Account Representative. Customers can also review SOC, ISO, PCI, and other audit reports directly through the Microsoft Service Trust Portal at http://aka.ms/audits.
AAC-02.2: Audit Assurance & Compliance - Independent Audits	*Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?*	Y			As defined in AIS-01.1, regular scans, conducted at least quarterly, are conducted against the Azure infrastructure and applications using a variety of commercial and proprietary scanning tools. Critical and High findings detected are reviewed and patched per the Change and Release Management Policy. Rescans are conducted within 30 days. Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state restoration.

AAC-02.3: Audit Assurance & Compliance - Independent Audits	*Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?*	Y			Scans are performed by MCIO security professionals on behalf of Microsoft Azure. Penetration testing methodologies for Infrastructure and Applications are defined and are based on a combination of common criteria, NIST SP800-115, ETSI, OWASP, IETF and ISO 27000. To protect Azure platform services, Microsoft provides a distributed denial-of-service (DDoS) defense system that is part of Azure's continuous monitoring process, and is continually improved through scheduled penetration-testing and Red-Team exercises. Azure's DDoS defense system is designed to mitigate attacks from the outside and also from other Azure tenants. The Azure DDoS defense technology provides detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits to help ensure that such attacks do not impact customer environments.
AAC-02.4: Audit Assurance & Compliance - Independent Audits	*Do you conduct internal audits regularly as prescribed by industry best practices and guidance?*	Y			Internal audits required to satisfy industry best practices, regulatory requirements and compliance requirements are conducted at the recommended intervals. Microsoft Azure complies with and audits against ISO 27001 controls in order to ensure that compliance is independently verified. The purpose of the internal audits is to assess conformance to the requirements of ISO 27001 and relevant legislation or regulations and to verify the identified information security requirements are effectively implemented and maintained.
AAC-02.5: Audit Assurance & Compliance - Independent Audits	*Do you conduct external audits regularly as prescribed by industry best practices and guidance?*	Y			Yes. Microsoft conducts audits and assessments against a growing number of US, international, and industry standards and frameworks. These include PCI DSS, SOC, ISO, IRAP, CDSA, MTCS, FedRAMP, DISA, and many others. More details about Azure's current portfolio of certifications can be found at the Azure Trust Center website.
AAC-02.6: Audit Assurance & Compliance - Independent Audits	*Are the results of the penetration tests available to tenants at their request?*	Y			Yes, summary penetration testing reports are available to customers under NDA. For more information, visit the Microsoft Azure Trust Center, or contact your Microsoft account representative.
AAC-02.7: Audit Assurance & Compliance - Independent Audits	*Are the results of internal and external audits available to tenants at their request?*	Y			The results of external audits are available publically on the Microsoft Azure Trust Center website; and some details of these reports are additionally available to customers with a signed NDA. Internal audits and their findings may contain sensitive information and are not made available.
AAC-02.8: Audit Assurance & Compliance - Independent Audits	*Do you have an internal audit program that allows for cross-*	Y			Microsoft conducts a variety of regular internal audits that are utilized in multiple different security and compliance assessments.

	functional audit of assessments?				
AAC-03.1: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?*	Y			Customer environments and data in Azure are isolated using numerous mechanisms, technologies, policies, processes, and architectural elements. Among these are (but not limited to): Virtual Networks--customer tenants and VM deployments are kept logically separated through VNets that define DNS, security policies, and IP routing rules. Firewalls, ACLs, Network Security Groups, IP Filters, Virtual appliances, Load Balancers, and network policies work together to prevent unauthorized traffic from entering or leaving a customer's tenant, either across network boundaries or between the virtualization host and guest. Encryption--customer data is encrypted in-transit and at-rest through configurable and standards-based providers using a variety of protocols. This includes BitLocker, AES-256 (in Azure Media Services), IPsec (VNets), etc. Access Control--Azure Storage, the Azure Portal, and other service components provide role-based access controls and key-based authentication to help ensure only authorized entities can gain access to tenant data. The concept of tenant containers is maintained in the Azure Active Directory service at multiple layers, from portals to persistent storage. These boundaries ensure a query scoped to a given tenant never returns directory data for another tenant. Front ends (Azure AD Sync, PowerShell, Graph) all store and retrieve data through an internal directory services API (DSAPI) which calls an authorization layer to ensure the data requested is allowed for the user requesting the data. All of these capabilities are available to customers for isolating and protecting their data, gaining access to only their data and no others'.
AAC-03.2: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have capability to recover data for a specific customer in the case of a failure or data loss?*	Y			Azure Storage automatically replicates your data to help guard against unexpected hardware failures and ensure that your data is available when you need it. Azure keeps 3 copies within a single region. For higher availability and disaster recovery, optional geo-redundancy creates 3 additional copies hundreds of miles away. When you create a storage account, you must select one of the following replication options: • **Locally redundant storage (LRS)** replicates your data within the region in which you created your storage account. To maximize durability, every request made against data in your storage account is replicated three times. These three replicas each reside in separate fault domains and upgrade domains.

					• **Zone-redundant storage (ZRS)** replicates your data across two to three facilities, either within a single region or across two regions, providing higher durability than LRS. If your storage account has ZRS enabled, then your data is durable even in the case of failure at one of the facilities. • **Geo-redundant storage (GRS)** replicates your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable. • **Read-access geo-redundant storage (RA-GRS)** providing read-only access to the data in the secondary location, in addition to the replication across two regions provided by GRS. In the event that data becomes unavailable in the primary region, your application can read data from the secondary region.
AAC-03.3: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?*	Y			Most Azure services are deployed regionally and enable the customer to specify the region of the Microsoft datacenter in which customer data will be stored, i.e. virtual machines, storage, and SQL Database. Data and VMs may be geo-tagged to prevent migration to locations not desired by the tenant. Data in Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Microsoft Azure Portal.
AAC-03.4: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?*	Y			Microsoft takes a two-pronged approach to help ensure that compliance controls are current and that we build and maintain a dynamic compliance framework. First, a team of Microsoft experts works with our engineering and operations teams, as well as external regulatory bodies, to track existing standards and regulations, developing hundreds of controls for our product teams to build into our cloud services. Second, because regulations and standards are always evolving, our compliance experts also anticipate upcoming changes to help ensure continuous compliance—researching draft regulations, assessing potential new requirements, and developing corresponding controls. This approach to designing compliance controls helps ensure that they operate effectively, with stringent safeguards.

Business Continuity Management and Operational Resilience: Controls BCR-01 through BCR-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
BCR-01.1: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with geographically resilient hosting options?*	Y			Yes. Most Azure services within larger geographies are deployed regionally and enable the customer to specify the region of the Microsoft datacenter in which customer data will be stored. The United States has 6 regions; Europe has 2 regions; Asia Pacific has 2 regions; Japan has two regions; Brazil has 1 region; and Australia has 2 regions. Azure creates three copies of data in the region configured by the customer and offers geo-replication in a datacenter hundreds of miles away within the same region.
BCR-01.2: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with infrastructure service failover capability to other providers?*		N		No, however, tenants have multiple options within the Azure platform to ensure workloads and data can have redundancy through mirroring and cold standby database failover capabilities, and interoperability with third party backup services if the customer so chooses.
BCR-02.1: Business Continuity Management & Operational Resilience - Business Continuity Testing	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?*	Y			BCPs have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RPO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.
BCR-03.1: Business Continuity Management & Operational Resilience - Datacenter Utilities /	*Do you provide tenants with documentation showing the transport route of their data between your systems?*	Y			Physical network diagrams are maintained for all Azure datacenters, with general data flow indicated in the System Descriptions that accompany the SOC 1, 2 and 3 audit reports. These diagrams provide functional level detail on load balancers, routers, firewalls, and other network infrastructure. SOC audit reports are available to customers under NDA from http://aka.ms/stphelp.

Environmental Conditions					
BCR-03.2: Business Continuity Management & Operational Resilience - Datacenter Utilities / Environmental Conditions	*Can tenants define how their data is transported and through which legal jurisdictions?*	Y			Customers may specify the geographic areas ("geos" and "regions") of the Microsoft datacenters in which their customer data will be stored, which allows for data being maintained in a particular jurisdiction. For example, to allow for the continuous flow of information required by international business (including the cross-border transfer of personal data), Microsoft offers customers EU Standard Contractual Clauses that provide additional contractual guarantees around transfers of personal data for in-scope services. Our implementation of the EU Model Clauses has been validated by EU data protection authorities as being in line with the rigorous privacy standards that regulate international data transfers by companies operating in its member states. Microsoft was the first company to receive approval from the EU's Article 29 Working Party for its strong contractual commitments to comply with EU privacy laws no matter where data is located.
BCR-04.1: Business Continuity Management & Operational Resilience - Documentation	*Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?*	Y			Extensive documentation, including operating procedures, security and hardening guides, diagrams, and system build documentation is maintained in a secure internal site and made available to authorized personnel. In addition, Microsoft Azure has established Security on-boarding SharePoint sites, assigned Privacy Champions and designated a Security team to provide guidance on security requirements. Access to system documentation is restricted to the respective Microsoft Azure teams based on their job roles.
BCR-05.1: Business Continuity Management & Operational Resilience - Environmental Risks	*Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?*	Y			Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

BCR-06.1: Business Continuity Management & Operational Resilience - Equipment Location	*Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?*		N		Microsoft data center site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where the exists a higher probability of earthquakes, seismic bracing of the facility is employed. Data centers are built as redundant, highly-available components of the Azure platform. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
BCR-07.1: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?*	Y			Underlying virtual hard disks (.vhd files) used by virtual machines are kept in Blob storage in an Azure storage account. Without additional configuration, data is protected by locally redundant storage, which maintains multiple replicas of data within a single region. If geo-replication for the virtual machine is configured, that geo-replication provides redundancy of data across regions to help ensure access to data in the event of a local disaster. Resource allocation is managed by Azure Fabric Controllers; Azure provides a combination of resource management, elasticity, load balancing, and partitioning to enable high availability. Azure services have redundant components; if one experiences a hardware failure or must be temporarily taken down to upgrade its software, the service remains available through other instances.
BCR-07.2: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?*	Y			Azure Backup provides the ability to back up and restore virtual machines. When the process to discover virtual machines in a region is initiated, a one-time registration is performed to install the backup extension, then a backup and retention policy is defined for each VM. From that point forward, replication and incremental backup is automatically performed. Once backed up, a VM can be restored from the latest recovery point or older, restore to an existing or new cloud service, and specify the virtual network and subnet for the restored VM.
BCR-07.3: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?*	Y			Within PowerShell, the Export-AzureVM command exports the state of an Azure virtual machine to a file. You can also use Azure Import/Export service to transfer large quantities of data resident in Blob storage to your on-premises installations.

BCR-07.4: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?*	Y			Customers may export virtual hard disk files and store those images outside of Azure.
BCR-07.5: Business Continuity Management & Operational Resilience - Equipment Maintenance	*Does your cloud solution include software/provider independent restore and recovery capabilities?*	Y			Tenants may use Azure Backup or StorSimple, which are services available to Azure customers, or they may utilize independent third party provider backup solutions to locations outside of the Azure platform.
BCR-08.1: Business Continuity Management & Operational Resilience - Equipment Power Failures	*Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?*	Y			Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, our network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. More importantly, we are continuously investing in developing greater application resiliency in our software so it will instantly recognize a disruption and gracefully failover to a different set of servers or even a different datacenter, without interrupting the availability of the service. Azure data centers have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators and data centers have made arrangements for emergency fuel delivery. Data centers also have a dedicated Facility Operations Center to monitor the following: Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.
BCR-09.1: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide tenants with ongoing visibility and reporting of your operational Service Level*	Y			Microsoft requires that customers submit an SLA breach claim to customer support by the end of the calendar month after the event has happened. (For example, if an incident happens in mid-February, the customer has until the end of March to report it.) The claim must include: a detailed description of the incident; duration of incident; number of users or sites impacted; description of your attempts to remedy the situation.

	Agreement (SLA) performance?				See also https://azure.microsoft.com/en-us/status/ for current status across all Azure datacenters and services.
BCR-09.2: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?*	Y			The security logs in Microsoft Azure Cloud Services and Virtual Machines contain vital information that can provide intelligence and insights into the following security issues including, policy violations, internal and external threats, regulatory compliance and network, host, and user activity anomalies. Customers can then use HDInsight to aggregate and analyze the collected events. In addition, these collected events can be exported to on-premises security information and event management (SIEM) systems for ongoing monitoring.
BCR-09.3: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide customers with ongoing visibility and reporting of your SLA performance?*	Y			Logs for primary operations related to your Azure subscription resources are also available through the Operation Logs feature in the Azure management portal. Microsoft monitors SLA performance and notifies customers if there is a lapse.
BCR-10.1: Business Continuity Management & Operational Resilience - Policy	*Are policies and procedures established and made available for all personnel to adequately support services operations' roles?*	Y			Management has established roles and responsibilities to oversee implementation of the information security policy across Microsoft Azure. Microsoft Azure management is responsible for overseeing security within their respective teams (including third parties), and facilitating compliance with security policies, processes and standards. In addition, Azure has established a Security on-boarding SharePoint site, assigned Privacy Champions and designated a Security team to provide guidance on security requirements. Access to system documentation is restricted to the respective Microsoft Azure teams based on their job roles. An Enterprise Business Continuity Management (EBCM) framework has been established for Microsoft and applied to individual business units including the Cloud and Enterprise (C&E) division under which Azure falls. The designated C&E Business Continuity Program Office (BCPO) works with Microsoft Azure management to identify critical processes and assess risks. The C&E BCPO provides guidance to the Microsoft Azure teams on EBCM framework and BCM roadmap, which includes the following components: • Governance; • Impact Tolerance;

					• Business Impact Analysis; • Dependencies Analysis (Non-Technical and Technical); • Strategies; • Planning; • Testing; and • Training and Awareness.
BCR-11.1: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements. The Microsoft Azure backup and redundancy program undergoes an annual review and validation and Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Customers are responsible for enforcing their own data retention policies, but Azure provides a 90-day window for subscription and storage account deletion to prevent accidental data loss. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location removal of any geo-replicated copy of the data (index) asynchronously, wiping is NIST 800-88 compliant, defective disks are destroyed, and customers can only read from disk space to which they have previously written.
BCR-11.2: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have a documented procedure for responding to requests for tenant data from governments or third parties?*	Y			Microsoft does not provide any government with direct or unfettered access to customer data. Microsoft releases only specific data mandated by the relevant legal demand. If a government wants customer data—including for national security purposes—it needs to follow the applicable legal process, meaning it must serve us with a court order for content or a subpoena for account information. If compelled to disclose customer data, we will promptly notify you and provide a copy of the demand, unless legally prohibited from doing so. We respond only to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, which ensures that the requests are valid, rejects those that are not, and makes sure that we provide only the data specified in the order. In its commitment to transparency, Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of government requests we receive. It is worth noting that the aggregate data we have published shows clearly that only a tiny fraction—fractions of a percent—of our customers have ever been subject to a government demand related to criminal law or national security. For enterprise customers, these numbers drop further to a mere handful.

					These privacy commitments are backed by Microsoft's adoption of the world's first international code of practice for cloud privacy, ISO/IEC 27108, in February 2015—the first major cloud provider to do so.
BCR-11.3: Business Continuity Management & Operational Resilience - Retention Policy	*Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?*	Y			Microsoft Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Backup standards and policies, procedures and controls are verified, documented and audited both internally and by third party assessors.
BCR-11.4: Business Continuity Management & Operational Resilience - Retention Policy	*Do you test your backup or redundancy mechanisms at least annually?*	Y			Yes, as defined in the Azure Business Continuity and Disaster Recovery Standard Operating Procedure.
BCR-11.5: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			Data retention policies and procedures are defined and maintained in accordance to regulatory, statutory, contractual or business requirements. The Microsoft Azure backup and redundancy program undergoes an annual review and validation and Azure backs up infrastructure data regularly and validates restoration of data periodically for disaster recovery purposes. Customers are responsible for enforcing their own data retention policies, but Azure provides a 90-day window for subscription and storage account deletion to prevent accidental data loss. Microsoft Azure provides tools to securely delete data including immediately removing the index from the primary location removal of any geo-replicated copy of the data (index) asynchronously, wiping is NIST 800-88 compliant, defective disks are destroyed, and customers can only read from disk space to which they have previously written.

Change Control & Configuration Management: Controls CCC-01 through CCC-05

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
CCC-01.1: Change Control & Configuration Management - New Development / Acquisition	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?*	Y			Microsoft follows NIST guidance regarding security considerations in software development in that information security must be integrated into the SDLC from system inception. Continual integration of security practices in the Microsoft SDL enables early identification and mitigation of security vulnerabilities and misconfigurations; awareness of potential software coding challenges caused by required security controls; identification of shared security services and reuse of security best practices tools which improving security posture through proven methods and techniques; and enforces Microsoft's already comprehensive risk management program. Microsoft Azure has established software development and release management processes to control implementation of major changes including: • The identification and documentation of the planned change • Identification of business goals, priorities and scenarios during product planning • Specification of feature/component design • Operational readiness review based on a pre-defined criteria/check-list to assess overall risk/impact • Testing, authorization and change management based on entry/exit criteria for DEV (development), INT (Integration Testing), STAGE (Pre-production) and PROD (production) environments as appropriate Customers are responsible for their own applications hosted in Microsoft Azure.
CCC-01.2: Change Control & Configuration Management - New Development / Acquisition	*Is documentation available that describes the installation, configuration and use of products/services/features?*	Y			Extensive documentation is available in the form of websites, whitepapers, Microsoft employee blog entries and video tutorials that describes the installation, configuration and use of products and features on the Azure website. Reference websites provide the most current information, documentation, video-on-demand, and procedures for configuring services in Compute, Web & Mobile, Data & Storage, Analytics and Networking.

CCC-02.1: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to ensure that standards of quality are being met for all software development?*	Y			External business partners are required to follow the same established software development and release management processes, including SDL and OSA guidelines, to control implementation of major changes as Microsoft Azure software developers. Microsoft also adheres to the SD3+C principle of development: Secure by design; Secure by default; secure in deployment and communications. Azure is also audited against the controls in the NIST 800-53 risk management framework which encompass quality control for FedRAMP.
CCC-02.2: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to detect source code security defects for any outsourced software development activities?*	Y			The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. Any outsourced software development follows the same controls and processes listed in CCC-01.1 and Microsoft Azure software changes are reviewed for unauthorized changes and defects through Security Development Lifecycle (SDL) change and release management processes.
CCC-03.1: Change Control & Configuration Management - Quality Testing	*Do you provide your tenants with documentation that describes your quality assurance process?*	Y			Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world. Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them. The foundation of secure online services consists of the following elements: - SDL, to ensure the software that underlies the service is designed and developed with security in mind throughout its entire lifecycle. - OSA, to ensure the deployment and operation of the service includes effective security practices throughout its lifecycle. The OSA process also uses feedback from online service teams within Microsoft to continuously evaluate and improve the OSA process. This feedback is also considered confidential, and it is protected in accordance with Microsoft internal policies. The three key processes of OSA are: - Ensuring that OSA inputs (such as organizational learning, threat intelligence, and security technologies) are up-to-date and relevant. - Developing and applying centralized review processes to

					consolidate all requirements to establish the OSA baseline requirements. - Engaging and implementing the new requirements and baselines. Customers also have access to third party audit reports and certifications that encompass the controls relevant to security in development and support processes which encompass quality assurance.
CCC-03.2: Change Control & Configuration Management - Quality Testing	*Is documentation describing known issues with certain products/services available?*	Y			Documentation of known issues with products and services are available at the Microsoft support website and within the Azure reporting platform.
CCC-03.3: Change Control & Configuration Management - Quality Testing	*Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?*	Y			Microsoft Azure identifies, reports, and corrects bugs and vulnerabilities through its incident response, vulnerability management and configuration management processes. Software updates to correct flaws are tested throughout the SDL process.
CCC-03.4: Change Control & Configuration Management - Quality Testing	*Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?*	Y			Prior to release to production, software code is inspected and reviewed during the quality assurance phase to ensure it is consistent with the approved build release. The engineer submits the code review to the internal review service, which creates the package of the changes and submits them for review. Project teams perform security testing in the implementation, verification and release phases of the Microsoft SDL process, including by employing automated code scanning and security tools to identify flaws and weaknesses in software. The identified flaws and vulnerabilities are formally tracked and remediated. When the code review is submitted, the system sends an email to the assigned reviewers and posts the code on the review site. An internal website is used as the hub for code submitted for review. As reviewers complete their reviews the details are stored on the server and the code owner is notified. Once approved, the code is queued.
CCC-04.1: Change Control & Configuration Management - Unauthorized Software Installations	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?*	Y			All changes into production go through the Change Management process described in CCC-01. This process also requires that: - Pre-screened admin requests from Microsoft corporate networks are approved - That role-based and Just-in-Time access controls are enforced - Privileges issued are temporary and grant the least privilege required to complete task (just-enough access)

					- Multi-factor authentication for all administrative access is required - All access requests are logged and audited Microsoft Azure source code libraries are limited to authorized personnel. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Azure and Microsoft Azure Contractors are granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained. “Access control and access control to program source code” is covered under the ISO 27001 standards, specifically addressed in Annex A, domains 11 and 12.4.3. For more information, review of the publicly available ISO standards we are certified against is suggested.
CCC-05.1: Change Control & Configuration Management - Production Changes	*Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?*	Y			Customers have access to third party audit reports and certifications that encompass the controls relevant to change management. Customers also receive their roles, rights and responsibilities in the Azure Terms & Conditions.

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
DSI-01.1: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?*		N		Microsoft Azure classifies data according to the Microsoft Azure data classification scheme and then implements a standard set of Security and Privacy attributes. Microsoft does not classify data uploaded and stored by customers.
DSI-01.2: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?*		N		All hardware is uniquely identified using software monitoring tools and hardware asset tags as part of the Azure Data Classification program. This data is not available to customers.
DSI-01.3: Data Security & Information Lifecycle Management - Classification	*Do you have a capability to use system geographic location as an authentication factor?*	Y			While geo-location cannot solely be used as an authentication factor, authentication can be restricted through the application of access control lists by IP addresses in specific geographies. Customers can generate reports from Azure AD and view anomalous login activity that could indicate a remote hacking attempt.
DSI-01.4: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location/geography of storage of a tenant's data upon request?*		N		Data in Microsoft Azure is stored in Microsoft datacenters around the world based on the geo-location properties specified by the customer using the Microsoft Azure Portal. While Azure can verify the geo or region in which data is located, it cannot provide the specific server or data center upon customer request.

DSI-01.5: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location / geography of storage of a tenant's data in advance?*	Y			Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area or region for redundancy, but it will not be replicated outside of it unless specifically configured so by the customer.
DSI-01.6: Data Security & Information Lifecycle Management - Classification	*Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?*	Y			Microsoft Azure classifies and labels data according to the Microsoft Azure data classification scheme and then implements a standard set of Security and Privacy attributes. Information classification, labeling and handling is covered under the ISO 27001:2013 standards, specifically addressed in domain 8.2.2.
DSI-01.7: Data Security & Information Lifecycle Management - Classification	*Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?*	Y			Most Azure services permit customers to specify the particular geography where their customer data will be stored and where their virtual machines are deployed. Virtual Networks (VNETS) may also span an entire region.
DSI-02.1: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?*	Y			Internally, Microsoft tracks data flows and network connectivity among its facilities worldwide. Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data, including through the use of: -- Features that do not enable geo selection such as Content Delivery Network (CDN) that provides a global caching service; -- Web and Worker Roles, which backup software deployment packages to the United States regardless of deployment geo; -- Preview, beta, or other pre-release features that may store or transfer Customer Data to the United States regardless of deployment geo; -- Azure Active Directory (except for Access Control), which may store Active Directory Data globally except for the United States (where Active Directory Data remains in the United States) and Europe (where Active Directory Data is in Europe and the United States); -- Azure Multi-Factor Authentication, which stores authentication data in the United States; -- Azure RemoteApp, which may store end user names and device IP addresses globally, depending on where the end user accesses the service.

DSI-02.2: Data Security & Information Lifecycle Management - Data Inventory / Flows	*Can you ensure that data does not migrate beyond a defined geographical residency?*	Y			Customers may specify the geo and region of the Microsoft datacenters where their data will be stored. Microsoft will not transfer data outside the geo(s) specified by the customer except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where the customer configures the account to enable the transfer of data, including through the use of features that don't enable geo selection or certain other features which may store data globally. A customer can access its data from any geo.
DSI-03.1: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?*	Y			Transactions involving the Microsoft Azure Portal, including purchase of services, is encrypted using TLS 1.2 256-bit encryption. SSL/TLS is mandatory when accessing the Azure Portal or System Management API (SMAPI). Microsoft Azure complies with PCI-DSS standards and completes an annual PCI audit by an independent, 3rd party PCI-DSS Qualified Security Assessor company. Azure customers are entirely responsible for protection and encryption of their e-commerce transactions, however, Azure ensures critical communications such as calls to the API or intra-Microsoft Azure communication are encrypted, authenticated, and integrity controlled via protocols such as SSL. Customers can optionally configure SSL/TLS for defense-in-depth on their Virtual Networks. Storage REST API over HTTPS can also be used to interact with Azure Storage and Azure SQL Database. When populating data into Azure SQL Database, you can encrypt information before it is copied over, or you can use Column Level Encryption / Transparent Data Encryption within the Azure SQL Database service. Note that data only remains encrypted until it is used and placed in memory on the Azure SQL Database compute node, at which point it exists in an unencrypted state.
DSI-03.2: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?*	Y			For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft data centers, and within data centers themselves.

DSI-04.1: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Are policies and procedures established for labeling, handling and the security of data and objects that contain data?*	Y			Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. The Asset Classification Standard and Asset Protection Standard describe the minimum security requirements that employees must apply to information assets based on their classification. All employees, contractors and third parties responsible for managing and maintaining assets must ensure that assets are handled securely and provided with appropriate level of protection.
DSI-04.2: Data Security & Information Lifecycle Management - Handling / Labeling / Security Policy	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?*	Y			Media and assets are marked as having a high/medium/low business impact which determines the level of security controls and handling procedures applicable. All media and assets are labeled without exception.
DSI-05.1: Data Security & Information Lifecycle Management - Non-Production Data	*Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?*	Y			The Azure platform is specifically designed and architected to prevent the possibility of production data being moved or replicated outside of the Azure cloud environment. These controls include: - Physical and logical network boundaries with strictly enforced change control policies - Segregation of duties requiring a business need to access an environment - Highly restricted physical and logical access to the cloud environment - Strict controls based on SDL and OSA that define coding practices, quality testing and code promotion - Ongoing security, privacy and secure coding practices awareness and training - Continuous logging and audit of system access - Regular compliance audits to ensure control effectiveness Microsoft Azure customers are responsible for defining policies and establishing controls for how their production data is maintained with regard to replication or high-availability and the demarcation of their production environment.
DSI-06.1: Data Security & Information Lifecycle Management - Ownership / Stewardship	*Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?*	Y			MCIO assets have a designated owner who is responsible for asset classification and protection in accordance with classification. Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets. Customers are considered the owners of their data as it exists in Azure.

					Azure assets are classified in accordance with Microsoft Online Services Classification Guidelines. Azure has conducted security categorization for its information and information systems and the results are documented, reviewed and approved by the authorizing official.
DSI-07.1: Data Security & Information Lifecycle Management - Secure Disposal	*Do you support secure deletion (e.g., degaussing / cryptographic wiping) of archived and backed-up data as determined by the tenant?*	Y			Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.
DSI-07.2: Data Security & Information Lifecycle Management - Secure Disposal	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?*	Y			Access to administer Microsoft Azure Active Directory portal/services is restricted based on assigned privileges and associated subscription of the customer account. When approved for deletion, the procedures outlined in DSI-07.1 are followed to remove customer data. See also http://blogs.msdn.com/b/walterm/archive/2012/02/01/windows-azure-data-cleansing-and-leakage.aspx.

Datacenter Security: Controls DCS-01 through DCS-09

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
DCS-01.1: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?*	Y			Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Asset owners are responsible for maintaining up-to-date information regarding their assets.
DCS-01.2: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical supplier relationships?*	Y			All critical supplier relationships are documented and reviewed at least annually or as changes occur to the relationship.
DCS-02.1: Datacenter Security - Controlled Access Points	*Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?*	Y			Microsoft datacenters are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates. Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities. CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities. Microsoft data centers all receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified
DCS-03.1: Datacenter Security - Equipment Identification	*Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?*	Y			MCIO, and consequently Azure, maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies of device configuration by comparing them against the defined policies. MCIO turns off the unused ports by default to prevent unauthorized access. Microsoft Azure Fabric Controlled Hardware Device Authentication maintains a set of credentials (keys and/or passwords) used to authenticate itself to various Microsoft Azure hardware devices under its control. The system used for

					transporting, persisting, and using these credentials is designed to make it unnecessary for Microsoft Azure developers, administrators, and backup services/personnel to be exposed to secret information.
DCS-04.1: Datacenter Security - Off-Site Authorization	*Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)*	Y			Microsoft asset and data protection procedures provide prescriptive guidance around the protection of logical and physical data and include instructions addressing relocation. Customers control where their data is stored while using Azure services such as Site Recovery and Backup.
DCS-05.1: Datacenter Security - Off-Site Equipment	*Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?*	Y			Data destruction techniques vary depending on the type of data object being destroyed, whether it be subscriptions, storage, virtual machines, or databases. In Azure's multi-tenant environment, careful attention is taken to ensure that one customer's data is not allowed to either "leak" into another customer's data, or when a customer deletes data, no other customer (including, in most cases, the customer who once owned the data) can gain access to that deleted data. Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.
DCS-06.1: Datacenter Security - Policy	*Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?*	Y			Microsoft Information Security policy defines and establishes controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized Microsoft personnel.

DCS-06.2: Datacenter Security - Policy	*Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?*	Y			All appropriate Microsoft employees take part in a Microsoft Azure sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. Microsoft also has non-disclosure provisions in our employee contracts. All Microsoft Azure contractor staff and MCIO staff are required to take any training determined to be appropriate to the services being provided and the role they perform.
DCS-07.1: Datacenter Security - Secure Area Authorization	*Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?*	Y			Customers may specify the geo and region of the Microsoft datacenters where their data will be stored. Microsoft will not transfer data outside the geo(s) specified by the customer except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where the customer configures the account to enable the transfer of data, including through the use of features that don't enable geo selection or certain other features which may store data globally. A customer can access its data from any geo. Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.
DCS-08.1: Datacenter Security - Unauthorized Persons Entry	*Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?*	Y			Azure Employees and contractors must have a business need to enter a Microsoft data center and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis. Failure to abide by the Microsoft Datacenter security policies means instant dismissal for the employee.
DCS-09.1: Datacenter Security - User Access	*Do you restrict physical access to information assets and functions by users and support personnel?*	Y			Access to all Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges and all guests be escorted by authorized Microsoft personnel.

Encryption and Key Management: Controls EKM-01 through EKM-04

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
EKM-01.1: Encryption & Key Management - Entitlement	*Do you have key management policies binding keys to identifiable owners?*	Y			Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Azure service. Azure provides each subscription with an associated logical certificate store that enables automatic deployment of service-specific certificates, and to which customers can upload their own. Certificates used in Azure are x.509 v3 certificates and can be signed by another trusted certificate or they can be self-signed. The certificate store is independent of any hosted service, so it can store certificates regardless of whether they are currently being used by any of those services. These certificates and other credentials uploaded to Azure are stored in encrypted form.
EKM-02.1: Encryption & Key Management - Key Generation	*Do you have a capability to allow creation of unique encryption keys per tenant?*	Y			Using Azure Key Vault, tenants can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, you can import or generate keys in HSMs (keys never leave the HSM boundary). HSMs are certified to FIPS 140-2 level 2.
EKM-02.2: Encryption & Key Management - Key Generation	*Do you have a capability to manage encryption keys on behalf of tenants?*	Y			Through the use of Key Vault, Azure provides a service for customers to manage and safeguard their cryptographic keys used by cloud applications. Key Vault allows encrypts keys and secrets, such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords, by using keys that are protected by hardware security modules (HSMs). HSMs are certified to FIPS 140-2 level 2.
EKM-02.3: Encryption & Key Management - Key Generation	*Do you maintain key management procedures?*	Y			Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Microsoft Azure service.
EKM-02.4: Encryption & Key Management - Key Generation	*Do you have documented ownership for each stage of the lifecycle of encryption keys?*	Y			Azure customers may use Key Vault to manage their own cryptographic keys while Azure provides the secure hardware platform. Customers can: - Create or import a key or secret - Revoke or delete a key or secret - Authorize users or applications to manage or use keys and secrets

					- Configure key usage (for example, sign or encrypt) - Monitor key usage Microsoft has policies, procedures, and mechanisms established for effective key management to support encryption of data in storage and in transmission for the key components of the Azure service. For internal corporate data and transmission encryption, Microsoft has established procedures to manage cryptographic keys throughout their lifecycle (e.g., generation, distribution, revocation). Microsoft Azure uses Microsoft's corporate PKI infrastructure.
EKM-02.5: Encryption & Key Management - Key Generation	*Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?*		N		The Azure Key vault is a cryptographic key management service based on FIPS-validated hardware security modules.
EKM-03.1: Encryption & Key Management - Sensitive Data Protection	*Do you encrypt tenant data at rest (on disk/storage) within your environment?*	Y			Microsoft Azure does not encrypt all tenant data in storage by default. However, there are tools within Azure and third party tools that allow encryption of data in Azure storage. Customers may implement encryption at rest using .NET cryptographic services and BitLocker (for full volume encryption). For customers using Virtual Machines, additional options are available, including the Encrypting File System in Windows Server 2008 R2 (and above), Azure Rights Management Services, as well as Transparent Data Encryption (TDE) in SQL Server 2008 R2 (and above). When using Azure SQL Database, externally encrypted records cannot be queried using T-SQL (other than "retrieve all") and may require a schema change such as the introduction of surrogate keys to enable retrieval of specific records or ranges of records.
EKM-03.2: Encryption & Key Management - Sensitive Data Protection	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?*	Y			Customers may configure Azure to enable encryption-in-transit by configuring HTTPS endpoints. Customers using Virtual Machines who wish to encrypt traffic between Web clients and Web servers in their VMs can implement TLS. Other enhancements to network traffic security include using IPsec VPNs or ExpressRoute to encrypt direct communications between the customer's datacenter and Microsoft Azure. For Azure SQL Database, all communication to and from SQL Database requires encryption (TLS 1.1) at all times. For customers who are connecting with a client that does not validate certificates upon connection, the connection to SQL Database is susceptible to "man in the middle" attacks. It is the customer's responsibility to determine if they are susceptible to this type of attack. Certificates must use a minimum of 2048-bit encryption.

EKM-03.3: Encryption & Key Management - Sensitive Data Protection	*Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?*	Y			Azure supports the import of tenant-generated encryption keys through Azure Key Vault and may be performed through the Management Portal and programmatically via SMAPI
EKM-03.4: Encryption & Key Management - Sensitive Data Protection	*Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?*	Y			Azure has documented and communicated Standard Operating Procedures (SOPs) that provide implementation guidance to operational teams. The SOPs provide documentation establishing and defining Azure encryption management policies, procedures and guidelines, are published at designated internal locations, and are reviewed annually. Cryptographic controls are used for information protection within the Microsoft Azure platform based on the Microsoft Azure Cryptographic Policy and Key Management procedures. Additional information may be obtained through the Customer's Account Manager.
EKM-04.1: Encryption & Key Management - Storage and Access	*Do you have platform and data appropriate encryption that uses open / validated formats and standard algorithms?*	Y			Azure supports strong cryptography using standard, validated formats including AES-256, IPSec, 1024-bit Perfect Forward Secrecy (PFS) and FIPS-140-2. Azure allows a customer to manage their own keys using independent Azure services for key vaulting, off-cloud third party key vaulting, or their own off-premises key management solution. Using Azure Key Vault, tenants can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys that are protected by hardware security modules (HSMs). For added assurance, customers can import or generate keys in HSMs (keys never leave the HSM boundary). HSMs are certified to FIPS 140-2 level 2.
EKM-04.2: Encryption & Key Management - Storage and Access	*Are your encryption keys maintained by the cloud consumer or a trusted key management provider?*	Y			Azure supports both topologies.
EKM-04.3: Encryption & Key Management - Storage and Access	*Do you store encryption keys in the cloud?*	Y			For customers, Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. Azure Key Vault supports multiple key types and algorithms and enables the use of Hardware Security Modules (HSM) for high value customer keys. Microsoft Azure uses Microsoft's corporate PKI infrastructure

					which functions as the CA, Registration Authority, and provides directory services to manage keys and certificates. The PKI service is used to generate SSL certificates for client-server communications as an infrastructure identity. All SSL certificates are issued directly by Microsoft via SSLAdmin and have a 2048-bit key size with validity for two years.
EKM-04.4: Encryption & Key Management - Storage and Access	*Do you have separate key management and key usage duties?*	Y			Azure has established and implemented procedures to enforce segregation of key management and key usage duties. Azure key management encompasses the entire life cycle of cryptographic keys and has identified a method for establishing and managing keys in each management phase from generation, installation, storage, rotation and destruction.

Governance and Risk Management: Controls GRM-01 through GRM-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
GRM-01.1: Governance and Risk Management - Baseline Requirements	*Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?*	Y			Microsoft Azure production servers are inspected prior to installation in the production environment to ensure they are configured in compliance with baseline security and operational settings appropriate to the server's intended role.
GRM-01.2: Governance and Risk Management - Baseline Requirements	*Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?*	Y			Microsoft Azure has established baseline configuration standards and procedures are implemented to monitor for compliance against these baseline configuration standards.
GRM-01.3: Governance and Risk Management - Baseline Requirements	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?*	Y			Customers may create and upload a virtual hard disk (VHD) for use as their own image to create virtual machines in Azure.
GRM-02.1: Governance and Risk Management - Data Focus Risk Assessments	*Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?*	Y			Microsoft Azure performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. Azure also provides the multiple logging and monitoring mechanisms for their VMs, including Windows events themselves, that can be enabled programmatically via the monitoring and diagnostics service. The Azure Security Center provides a central view of the security state of Azure resources, to help verify that the appropriate security controls are in place and configured correctly.

GRM-02.2: Governance and Risk Management - Data Focus Risk Assessments	*Do you conduct risk assessments associated with data governance requirements at least once a year?*	Y			Microsoft Azure performs an annual risk assessment. As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. Microsoft Azure's controls for risk and vulnerability assessment of the Azure infrastructure encompass all areas in this section and meet the requirements of the standards against which the audit reports we have identified on the Azure website at: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
GRM-03.1: Governance and Risk Management - Management Oversight	*Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?*	Y			Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Staff for review. All Microsoft Azure Staff represent that they have reviewed, and agree to adhere to, all policies within the Policy documents. All Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Policy. Should one of these parties not have access to this policy for any reason, the supervising Microsoft agent is responsible for distributing the policy to them.
GRM-04.1: Governance and Risk Management - Management Program	*Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?*	Y			An overall ISMS for Microsoft Azure has been designed and implemented to address industry best practices around security and privacy. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.
GRM-04.2: Governance and Risk Management - Management Program	*Do you review your Information Security Management Program (ISMP) least once a year?*	Y			Microsoft Azure performs annual ISMS reviews, the results of which are reviewed by management. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.
GRM-05.1: Governance and Risk Management - Management Support / Involvement	*Do you ensure your providers adhere to your information security and privacy policies?*	Y			Each management-endorsed version of the Information Security Policy and all subsequent updates are distributed to all relevant stakeholders. The Information Security Policy is made available to all new and existing Microsoft Azure employees for review. Information roles and responsibilities are clearly defined and assigned, and management at all levels is responsible for ensuring policies are followed.

GRM-06.1: Governance and Risk Management - Policy	*Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?*	Y			Microsoft Azure has designed and implemented an ISMS framework that addresses industry best-practices for information security and privacy, based on open standards including ISO 27001, NIST 800-53 / 37, PCI DSS, and others. The ISMS has been documented and communicated in a customer-facing Information Security Policy, which can be made available upon request (customers and prospective customers must have a signed NDA or equivalent in place to receive a copy). This policy is reviewed and approved annually by Microsoft Azure management, who has established roles and responsibilities to oversee implementation of the policy. Microsoft Azure information security and privacy policies align with industry standards align with many industry standards and are described in the Azure Trust Center.
GRM-06.2: Governance and Risk Management - Policy	*Do you have agreements to ensure your providers adhere to your information security and privacy policies?*	Y			Yes. All Microsoft Azure Contractor Staff agree to adhere to the relevant policies within the Information Security Policy. Agreements are in place that specify security and privacy compliance requirements for all third party contractors. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts.
GRM-06.3: Governance and Risk Management - Policy	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?*	Y			All compliance documents reference a standard and can be verified by this document and others on the Azure Trust Center website. A customer facing version of the Information Security Policy can be made available upon request. Customers and prospective customers must have a signed NDA or equivalent in order to receive a copy of the Information Security Policy.
GRM-06.4: Governance and Risk Management - Policy	*Do you disclose which controls, standards, certifications and/or regulations you comply with?*	Y			Microsoft Azure provides a listing of all controls, standards, certifications and/or regulations complied with, both in publicly disclosed information on the Azure website and through security documents shared with customers available under NDA.
GRM-07.1: Governance and Risk Management - Policy Enforcement	*Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?*	Y			Microsoft Azure services staff suspected of committing breaches of security and/or violating the Information Security Policy equivalent to a Microsoft Code of Conduct violation are subject to an investigation process and appropriate disciplinary action up to and including termination. Contracting staff suspected of committing breaches of security and/or violations of the Information Security Policy are subject to formal investigation and action appropriate to the associated contract, which may include termination of such contracts.

					Human Resources is responsible for coordinating disciplinary response.
GRM-07.2: Governance and Risk Management - Policy Enforcement	*Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?*	Y			All employees are required to read and acknowledge the policies which detail possible actions in the event of a violation.
GRM-08.1: Governance and Risk Management - Policy Impact on Risk Assessments	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?*	Y			Microsoft Azure performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to the management through a formal risk assessment report. Microsoft Azure Risk Management organization bases the risk assessment framework on the ISO27001 standards. An integrated part of the methodology is the risk assessment process. Decisions to update policies and procedures are based on the risk assessment reports. Risk assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.
GRM-09.1: Governance and Risk Management - Policy Reviews	*Do you notify your tenants when you make material changes to your information security and/or privacy policies?*	Y			In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule. Changes to security and privacy policies which impact tenants are formally communicated to the designated point of contact.
GRM-09.2: Governance and Risk Management - Policy Reviews	*Do you perform, at minimum, annual reviews to your privacy and security policies?*	Y			The Microsoft Azure Information Security Policy undergoes a formal management review and update process at a regularly scheduled interval not to exceed 1 year.
GRM-10.1: Governance and Risk Management - Risk Assessments	*Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all*	Y			Azure performs an annual risk assessment. As part of the overall ISMS framework baseline security requirements are constantly being reviewed, improved and implemented. Microsoft Azure's controls for risk and vulnerability assessment of the Azure infrastructure encompass all areas in this section and meet the requirements of the standards against which the audit reports we have identified on the Azure website.

	identified risks, using qualitative and quantitative methods?				
GRM-10.2: Governance and Risk Management - Risk Assessments	*Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?*	Y			The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. According measures, recommendations and controls are put in place to mitigate the risks to the extent possible.
GRM-11.1: Governance and Risk Management - Risk Management Framework	*Do you have a documented, organization-wide program in place to manage risk?*	Y			The Risk Assessment program is in place throughout the Microsoft Azure and Microsoft enterprise. As part of this process, threats to security are identified and the risk from these threats is formally assessed. This involves monitoring ongoing effectiveness and improvement of the ISMS control environment by reviewing security issues, audit results, and monitoring status, and by planning and tracking necessary corrective actions.
GRM-11.2: Governance and Risk Management - Risk Management Framework	*Do you make available documentation of your organization-wide risk management program?*	Y			Risk management documentation is made available through the various published audit reports made available on the Azure Trust Center website.

Human Resources: Controls HRS-01 through HRS-11

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
HRS-01.1: Human Resources - Asset Returns	*Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?*	Y			Microsoft Corporate Human Resources Policy drives employee termination processes and in coordination with management, ensures all organizationally-owned assets are returned upon employee or contractor termination. Employees, contractors and third party users are formally notified to destroy or return, as applicable, any physical materials that Microsoft has provided to them during the term of employment or the period of Contractor agreement and any electronic media must be removed from Contractor or third party infrastructure. Microsoft may also conduct an audit to make sure data is removed in an appropriate manner.
HRS-01.2: Human Resources - Asset Returns	*Is your Privacy Policy aligned with industry standards?*	Y			Microsoft Azure is first major cloud provider to adopt the ISO 27018 privacy standard. Privacy Policy aligns with relevant statutory, regulatory and contractual requirements identified by Microsoft. Azure operates under the following five principles: **Consent:** CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing. **Control:** Customers have explicit control of how their information is used. **Transparency:** CSPs must inform customers where their data resides, disclose the use of subcontractors to process PII and make clear commitments about how that data is handled. Communication: In case of a breach, CSPs should notify customers, and keep clear records about the incident and the response to it. **Independent and yearly audit:** A successful third-party audit of a CSP's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, the CSP must subject itself to yearly third-party reviews.
HRS-02.1: Human Resources - Background Screening	*Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates,*	Y			Pursuant to local laws, regulations, ethics and contractual constraints, all Microsoft US-based full-time employees (FTE) are required to successfully complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.

	contractors and involved third parties subject to background verification?				
HRS-03.1: Human Resources - Employment Agreements	*Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?*	Y			All Microsoft Azure contractor staff and FTE staff are required to take any training determined to be appropriate, such as Microsoft Privacy 101, to the services being provided and the role they perform.
HRS-03.2: Human Resources - Employment Agreements	*Do you document employee acknowledgment of training they have completed?*	Y			All FTE and third-party training is tracked and verified.
HRS-03.3: Human Resources - Employment Agreements	*Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?*	Y			Microsoft Azure has established confidentiality and non-disclosure agreements for protection of customer information within its environment. Responsibilities are designated to validate that agreements include relevant confidentiality, privacy, and security requirements.
HRS-03.4: Human Resources - Employment Agreements	*Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?*	Y			Successful completion of required security and privacy training is required for all FTE and contractors granted access to sensitive systems.
HRS-03.5: Human Resources - Employment Agreements	*Are personnel trained and provided with awareness programs at least once a year?*	Y			All Microsoft Azure, Microsoft FTE and contractors are required to complete security and privacy training upon hire and annually thereafter. Security Awareness training is also provided in an ongoing basis through a variety of media.

HRS-04.1: Human Resources - Employment Termination	*Are documented policies, procedures and guidelines in place to govern change in employment and / or termination?*	Y			Microsoft Corporate Human Resources Policy drives employee termination processes and Microsoft Policy clearly defined roles and responsibilities. Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to all resources, both physical and electronic.
HRS-04.2: Human Resources - Employment Termination	*Do the above procedures and guidelines account for timely revocation of access and return of assets?*	Y			Termination policies and procedures cover all aspects of separation including return of assets, badges, computer equipment and data. Human Resources also manages revocation of access to all resources, both physical and electronic.
HRS-05.1: Human Resources - Mobile Device Management	*Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?*	Y			Microsoft Azure teams and personnel are required to adhere to applicable policies, which do not permit mobile computing devices to access the production environment, unless those devices have been approved for use by Microsoft Azure Management. Mobile computing access points are required to adhere with the wireless device security requirements.
HRS-06.1: Human Resources - Non-Disclosure Agreements	*Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and*	Y			Microsoft Legal and Human Resources maintain policies and procedures defining the implementation and execution of non-disclosure and confidentiality agreements. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire and annually thereafter. In addition, employees must acknowledge Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, on an annual basis.

	reviewed at planned intervals?				
HRS-07.1: Human Resources - Roles / Responsibilities	*Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?*	Y			Tenant roles and responsibilities are clearly defined in Azure policies which are acknowledged by tenants when subscribing to the service. The Information Security Policy exists in order to provide Microsoft Azure Staff and Contractor Staff with a current set of clear and concise Information Security Policies including their roles and responsibilities related to information assets and security. These policies provide direction for the appropriate protection of Microsoft Azure. The Information Security Policy has been created as a component of an overall Information Security Management System (ISMS) for Microsoft Azure. The Policy has been reviewed, approved, and is endorsed by Microsoft Azure management.
HRS-08.1: Human Resources - Technology Acceptable Use	*Do you provide documentation regarding how you may or access tenant data and metadata?*	Y			Customer Data will be used only to provide customer the Microsoft Azure service. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). More information on Microsoft's commitment around use of customer data can be found in the Privacy Statement and Online Services Use Rights at the reference sites.
HRS-08.2: Human Resources - Technology Acceptable Use	*Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?*		N		No. Azure does not share customer data with its advertiser-supported services, nor is customer data mined for marketing or advertising. This policy is backed by our enterprise cloud service agreements and reaffirmed by Microsoft's adoption of the international code of practice for cloud privacy, ISO/IEC 27018.
HRS-08.3: Human Resources - Technology Acceptable Use	*Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?*			N/A	Not applicable. Microsoft does not inspect customer subscription data.
HRS-09.1: Human Resources - Training / Awareness	*Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy,*	Y			All appropriate Microsoft employees take part in a Microsoft Azure sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. Microsoft also has non-disclosure provisions in our employee contracts. All Microsoft Azure contractor staff and MCIO staff are required

	nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?				to take any training determined to be appropriate to the services being provided and the role they perform.
HRS-09.2: Human Resources - Training / Awareness	*Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?*	Y			All data is designated with stewardship with assigned responsibilities defined, documented and communicated.
HRS-10.1: Human Resources - User Responsibility	*Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?*	Y			All Microsoft Azure personnel are made aware of their roles and responsibilities through the use of multiple methods including regular newsletters, posters, live and computer-based training, policies and internal meetings. Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire and annually thereafter. In addition, employees must acknowledge Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, on an annual basis.
HRS-10.2: Human Resources - User Responsibility	*Are users made aware of their responsibilities for maintaining a safe and secure working environment?*	Y			Yes. See HRS-10.1
HRS-10.3: Human Resources - User Responsibility	*Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?*	Y			Security policy defines requirements for secure operation of equipment, secure work areas, and policies regarding unattended equipment.
HRS-11.1: Human Resources - Workspace	*Do your data management policies and procedures address tenant and service*	Y			MCIO inherits the Microsoft corporate AD session lock functionality and enforces session lock outs after a defined period of inactivity. Terminal Server boundary protection devices limit the number of sessions that can be established to a MCIO host to one. Network connections are terminated after

	level conflicts of interests?				a defined period of inactivity. Conflict of interest definitions and FTE requirements are communicated and acknowledged by staff upon hire and at least annually thereafter.
HRS-11.2: Human Resources - Workspace	*Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?*	Y			Hardware and software integrity monitoring are in place and audited on a regular basis.
HRS-11.3: Human Resources - Workspace	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build / configuration of the virtual machine?*	Y			The Microsoft Azure platform provides automated logging and alerting capabilities for monitoring system use and detection of potential unauthorized activity.

Identity and Access Management: Controls IAM-01 through IAM-13

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IAM-01.1: Identity & Access Management - Audit Tools Access	*Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)*	Y			Log and monitor access is highly restricted to only authorized staff with a business need to access such systems. Microsoft Azure platform components (including OS, CloudNet, Fabric, etc.) are configured to log and collect security events.
IAM-01.2: Identity & Access Management - Audit Tools Access	*Do you monitor and log privileged access (administrator level) to information security management systems?*	Y			Per IAM-01.2, all access to log and monitor systems is monitored and audited.
IAM-02.1: Identity & Access Management - Credential Lifecycle / Provision Management	*Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?*	Y			Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azures' assets is granted based upon business requirements and with the asset owner's authorization. Additionally: • Access to assets is granted based upon need-to-know and least-privilege principles; all access is set to auto-expire on a preconfigured limit. • Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. • Physical and logical access control policies are consistent with standards. Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. The temporary passwords are communicated to the users using MSIT established processes. All services and infrastructure must at a minimum meet MSIT requirements but an internal organization can increase the

					strength past this standard, on their own discretion and to meet their security needs. It is the customer's responsibility to manage access to the Account Admin, Service Admin and Co-Admin roles within the Microsoft Azure portal.
IAM-02.2: Identity & Access Management - Credential Lifecycle / Provision Management	*Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?*	Y			Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity.
IAM-03.1: Identity & Access Management - Diagnostic / Configuration Ports Access	*Do you use dedicated secure networks to provide management access to your cloud service infrastructure?*	Yes			Microsoft Azure controls physical access to diagnostic and configuration ports through physical data center controls. Diagnostic and configuration ports are only accessible by arrangement between service/asset owner and hardware/software support personnel requiring access, using recommended secure administration workstations. Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL Azure services layer includes TDS gateways that control information flows through stateful inspection.
IAM-04.1: Identity & Access Management - Policies and Procedures	*Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?*	Yes			Access control policy is a component of overall policies and undergoes a formal review and update process. Access to Microsoft Azures' assets is granted based upon business requirements and with the asset owner's authorization. Additionally: • Access to assets is granted based upon need-to-know and least-privilege principles. • Where feasible, role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. • Physical and logical access control policies are consistent with standards. Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date.

					Domain-level user accounts are disabled after 90 days of inactivity. MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website.
IAM-04.2: Identity & Access Management - Policies and Procedures	*Do you manage and store the user identity of all personnel who have network access, including their level of access?*	Y			See IAM-04.1
IAM-05.1: Identity & Access Management - Segregation of Duties	*Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?*	Y			MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website.
IAM-06.1: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?*	Y			Microsoft Azure source code libraries are limited to authorized personnel. Where feasible, source code libraries maintain separate project work spaces for independent projects. Microsoft Azure and Microsoft Azure Contractors are granted access only to those work spaces which they need access to perform their duties. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained.
IAM-06.2: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to*	Y			Multiple physical, technical and logical controls are in place and monitored to prevent unauthorized access to restricted data.

	authorized personnel only?				
IAM-07.1: Identity & Access Management - Third Party Access	*Do you provide multi-failure disaster recovery capability?*	Y			Identification of risks related to external parties and access controls is performed as part of our Risk Management program and verified as part of our ISO 27001 audit. Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Microsoft Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.
IAM-07.2: Identity & Access Management - Third Party Access	*Do you monitor service continuity with upstream providers in the event of provider failure?*	Y			Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Microsoft Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.
IAM-07.3: Identity & Access Management - Third Party Access	*Do you have more than one provider for each service you depend on?*	Y			Based on risk and criticality, multiple service providers are engaged.
IAM-07.4: Identity & Access Management - Third Party Access	*Do you provide access to operational redundancy and continuity summaries, including the services you depend on?*	Y			Operation redundancy is in place for dependent services. Additional risks related to granting access to facilities and information systems are controlled and managed by MSIT.
IAM-07.5: Identity & Access Management - Third Party Access	*Do you provide the tenant the ability to declare a disaster?*	Y			Tenants may independently declare a disaster.

IAM-07.6: Identity & Access Management - Third Party Access	*Do you provide a tenant-triggered failover option?*	Y			Tenants may initiate failover mechanisms at their discretion.
IAM-07.7: Identity & Access Management - Third Party Access	*Do you share your business continuity and redundancy plans with your tenants?*		N		BCPs are documented and reviewed annually, and are attested by external auditors conducting compliance reviews for ISO, SOC, PCI, FedRAMP, and other standards.
IAM-08.1: Identity & Access Management - Trusted Sources	*Do you document how you grant and approve access to tenant data?*	Y			When granted, access is carefully controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed. Microsoft Azure uses Active Directory (AD) to manage user accounts. Security group membership must be approved by the designated security group owners within Microsoft Azure. Automated procedures are in place to disable AD accounts upon the user's leave date. Domain-level user accounts are disabled after 90 days of inactivity. MCIO enforces segregation of duties through user defined groups to minimize the risk of unintentional or unauthorized access or change to production systems. Information system access is restricted based on the user's job responsibilities. Documentation on how Microsoft Azure maintains segregation of duties is included in the available security framework audit results on the Azure Trust Center website.
IAM-08.2: Identity & Access Management - Trusted Sources	*Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?*		N		No. Data classification methodologies are not integrated, however, Azure platform data classification is designed to ensure tenant data classification policies are enforced when implemented.
IAM-09.1: Identity & Access Management - User Access Authorization	*Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or*	Y			Microsoft Azure has adopted applicable corporate and organizational security policies, including an Information Security Policy. The policies have been approved, published and communicated to Microsoft Azure personnel. The Information Security Policy requires that access to Microsoft Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access

	suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?				authorization, removal of access rights and periodic access reviews.
IAM-09.2: Identity & Access Management - User Access Authorization	*Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?*	Y			Where approved and authorized according to the Azure ISMS, user access to data or assets is granted.
IAM-10.1: Identity & Access Management - User Access Reviews	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?*	Y			The Information Security Policy requires that access to Microsoft Azure assets to be granted based on business justification, with the asset owner's authorization and limited based on "need-to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews. Managers and owners of applications and data are responsible for reviewing who has access on a periodic basis. Privileged accounts are reviewed at least every three (3) months to ensure the privileged access level is still appropriate. Access is modified based on the results of the reviews. A quarterly review is performed by FTE managers to validate the appropriateness of access to MCIO-managed network devices. A quarterly review is performed by FTE managers and MCIO security group owners to validate the appropriateness of user access. Security group memberships are reviewed for appropriateness on a quarterly basis and access is modified based on the results of the review.

IAM-10.2: Identity & Access Management - User Access Reviews	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?*	Y			Procedures have been established to disable access for terminated or transferred users within 5 business days.
IAM-10.3: Identity & Access Management - User Access Reviews	*Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?*	Y			If tenant data was inappropriately accessed, tenants will be notified. Entitlement remediation and certification reports may be shared on a case by case basis.
IAM-11.1: Identity & Access Management - User Access Revocation	*Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?*	Y			Designated security group owners within Microsoft Azure are responsible for reviewing appropriateness of employee access to applications and data on a periodic basis. Regular access review audits occur to validate appropriate access provisioning has taken place. Access is modified based on the results of this review. Membership in security groups must be approved by security group owners. Automated procedures are in place to disable AD accounts upon the user's leave-date. Within the Microsoft Azure environment, customers are responsible for managing access to the applications customers host on Microsoft Azure.
IAM-11.2: Identity & Access Management - User Access Revocation	*Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?*	Y			Access permissions are reviewed and modified as appropriate during both a change in role or termination.

IAM-12.1: Identity & Access Management - User ID Credentials	*Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?*	Y			Password policies for corporate domain accounts are managed through Microsoft corporate Active Directory policy that specifies minimum requirements for password length, complexity and expiry. The temporary passwords are communicated to the users using MSIT established processes. All services and infrastructure must at a minimum meet MSIT requirements but an internal organization can increase the strength past this standard, on their own discretion and to meet their security needs. Customers are responsible for keeping passwords from being disclosed to unauthorized parties and for choosing passwords with sufficient entropy as to be effectively non-guessable and for deployment of services such as multi-factor authentication.
IAM-12.2: Identity & Access Management - User ID Credentials	*Do you use open standards to delegate authentication capabilities to your tenants?*	Y			Standards including SMAPI and REST APIs are supported.
IAM-12.3: Identity & Access Management - User ID Credentials	*Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?*	Y			Currently customers can manage their subscription by connecting to the Azure Management Portal over "https" or programmatically via REST API with their unique federated identity (customer domain AD user name and password). This grants the authenticated user with access to the connection string and administrator login and password for that particular Azure Subscription. Azure supports OpenID Connect, OAuth 2.0, and WS-Federation.
IAM-12.4: Identity & Access Management - User ID Credentials	*Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?*		N		Customers may control access using IP policies to prevent logins from certain regions.
IAM-12.5: Identity & Access Management - User ID Credentials	*Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?*	Y			Azure AD provides identity management and RBAC capabilities, but customers must configure policies and entitlements as dictated by their business needs.

IAM-12.6: Identity & Access Management - User ID Credentials	*Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?*	Y			Azure Multi-Factor Authentication helps safeguard access to data and applications, and delivers strong authentication with a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer. https://azure.microsoft.com/en-us/services/multi-factor-authentication/
IAM-12.7: Identity & Access Management - User ID Credentials	*Do you allow tenants to use third-party identity assurance services?*	Y			Customers may implement third party assurance solutions.
IAM-12.8: Identity & Access Management - User ID Credentials	*Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?*	Y			The creation and allocation of passwords and PINs are managed through the standard account management processes. Policies and standards have been established and implemented for password expiration, length, complexity and history.
IAM-12.9: Identity & Access Management - User ID Credentials	*Do you allow tenants/customers to define password and account lockout policies for their accounts?*	Y			Customers are responsible for configuring unsuccessful login settings for access via their enablers by: a. Enforcing a limit of 3 consecutive invalid access attempts by a user during a 15-minute interval; and b. Automatically locking the account for 30 minutes, locking the account until it is released by an administrator, or delaying the next login prompt for the organization's defined delay when the maximum number of unsuccessful attempts is exceeded.
IAM-12.10: Identity & Access Management - User ID Credentials	*Do you support the ability to force password changes upon first logon?*	Y			The customer sets the password for the Azure portal root account at time of account creation.
IAM-12.11: Identity & Access Management - User ID Credentials	*Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge*	Y			Microsoft Azure Active Directory password policy requirements are enforced on the new passwords supplied by customers within the AADUX portal. Customer initiated self-service password changes require validation of older password. Administrator reset passwords are required to be changed upon subsequent login.

	questions, manual unlock)?				
IAM-13.1: Identity & Access Management - Utility Programs Access	*Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?*	Y			Utility programs undergo changes and the release management process and are restricted to authorized personnel only. Administrative access and privileges to the Azure platform are restricted to authorized personnel through designated AD security groups based on job responsibilities. Security group membership must be approved by the designated security group owners within Microsoft Azure.
IAM-13.2: Identity & Access Management - Utility Programs Access	*Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?*	Y			A variety of software and hardware based technical controls are in place to detect attacks directed at Azure virtual infrastructure.
IAM-13.3: Identity & Access Management - Utility Programs Access	*Are attacks that target the virtual infrastructure prevented with technical controls?*	Y			A variety of technical controls are in place to prevent attacks including, but not limited to, Next-Generation firewalls, IDS/APS, network segmentation and network security analytics.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IVS-01.1: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?*	Y			Forefront Identity Manager and IDS tools are implemented within the Azure environment. Microsoft Azure uses and Early Warning System (EWS) to support real-time analysis of events within its operational environment. Monitoring Agents and the Azure Incident Management System generate near real-time alerts about events that could potentially compromise the system.
IVS-01.2: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Is physical and logical user access to audit logs restricted to authorized personnel?*	Y			MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on OSSC's secure archival infrastructure and are retained for 180 days.
IVS-01.3: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?*	Y			Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. MCIO restricts access to audit logs to authorized personnel based on job responsibilities. Event logs are archived on OSSC's secure archival infrastructure and are retained for 180 days. “Audit logging” is covered under the ISO 27001 standards and additional details can be found in the audit reports provided on the Azure Trust Center website.
IVS-01.4: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are audit logs centrally stored and retained?*	Y			Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally.
IVS-01.5: Infrastructure & Virtualization Security - Audit Logging / Intrusion Detection	*Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?*	Y			MCIO-managed network devices are configured to log and collect security events. The list of auditable events is reviewed and updated periodically or whenever there is a change in the systems' threat environment. MCIO has established monitoring systems to detect audit processing failures and report to appropriate personnel. Audit logs are stored for a minimum of 180 days.

IVS-02.1: Infrastructure & Virtualization Security - Change Detection	*Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?*	Y			Read and write operations to virtual machines are logged via storage analytics, which the customer can view within their own storage account. Azure Virtual Machines staged in the Azure Gallery are maintained according to established software asset management procedures, which includes update logs to stored VHDs.
IVS-02.2: Infrastructure & Virtualization Security - Change Detection	*Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?*	Y			Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process - SSIRP updates) are deployed as quickly as possible. If customers use the default "Auto Upgrade" option, software updates will be applied their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In case of a VM role, customers are responsible for evaluating and updating their VMs.
IVS-03.1: Infrastructure & Virtualization Security - Clock Synchronization	*Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?*	Y			MCIO has established procedures to synchronize servers and network devices in the Azure environment with NTP Stratum 1 time servers that sync off of the Global Positioning System (GPS) satellites. The synchronization is performed automatically every five minutes.
IVS-04.1: Infrastructure & Virtualization Security - Information System Documentation	*Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances / scenarios?*	Y			The following operational processes in place: -Proactive capacity management based on defined thresholds or events; -Hardware and software subsystem monitoring for acceptable service performance and availability, service utilization, storage utilization and network latency. Proactive monitoring continuously measures the performance of key subsystems of the Microsoft Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event. Customers are responsible for monitoring and planning the capacity needs of their applications.
IVS-04.2: Infrastructure & Virtualization	*Do you restrict use of the memory oversubscription*	Y			Customer VMs are prevented from oversubscribing memory resources by the Azure hypervisor, which only allocates as much memory as has been requested by the VM when it is

Security - Information System Documentation	*capabilities present in the hypervisor?*				instantiated. Azure does not allow VMs to write to more memory than is initially allocated.
IVS-04.3: Infrastructure & Virtualization Security - Information System Documentation	*Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?*	Y			Microsoft Azure Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams.
IVS-04.4: Infrastructure & Virtualization Security - Information System Documentation	*Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?*	Y			Proactive monitoring continuously measures the performance of key subsystems of the Microsoft Azure services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.
IVS-05.1: Infrastructure & Virtualization Security - Vulnerability Management	*Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?*	Y			Vulnerability assessment and scanning tools are specifically designed to operate in virtualized environments. Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices. The vulnerability scans are performed on a quarterly basis at a minimum. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Red-Team exercises are also routinely performed and results used to make security improvements.
IVS-06.1: Infrastructure & Virtualization Security - Network Security	*For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?*	Y			SQL Azure employs boundary protection devices such as SQL Azure Gateways, CGs, application firewalls and DOSGuard to control communications at external and internal boundaries. Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine any changes required. Security best practices and guidance on defense in depth are published on the Azure website.

IVS-06.2: Infrastructure & Virtualization Security - Network Security	*Do you regularly update network architecture diagrams that include data flows between security domains/zones?*	Y			Yes. Internal diagrams are updated at least annually or as changes are made to the network.
IVS-06.3: Infrastructure & Virtualization Security - Network Security	*Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?*	Y			Yes. All firewall rules and ACLs are documented and reviewed on at least a quarterly basis. All changes are required to follow the approved firewall rule change control process. Traffic flow policies are implemented on boundary protection devices that deny traffic by default. These policies are reviewed every month to determine any changes required.
IVS-06.4: Infrastructure & Virtualization Security - Network Security	*Are all firewall access control lists documented with business justification?*	Y			Yes. All firewall rules and ACLs are documented and reviewed on at least a quarterly basis. All changes are required to follow the approved firewall rule change control process.
IVS-07.1: Infrastructure & Virtualization Security - OS Hardening and Base Controls	*Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?*		N		It is a customer responsibility to harden any VM operating systems or templates. Microsoft Azure software and hardware configurations are reviewed at least quarterly to identify and eliminate any unnecessary functions, ports, protocols and services. Azure Anti-Malware Services are available on Azure Gallery OS images by default, but must be enabled by the customer.
IVS-08.1: Infrastructure & Virtualization Security - Production / Non-Production Environments	*For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?*	Y			Within the Azure platform, tenants define their own production and non-production environments. For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL

					Azure services layer includes TDS gateways that control information flows through stateful inspection.
IVS-08.2: Infrastructure & Virtualization Security - Production / Non-Production Environments	*For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?*	Y			Azure provides guidance on configuring multiple environments through web documentation, blogs, TechNet, diagrams, Video on Demand and through Azure web-based training.
IVS-08.3: Infrastructure & Virtualization Security - Production / Non-Production Environments	*Do you logically and physically segregate production and non-production environments?*	Y			For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL Azure services layer includes TDS gateways that control information flows through stateful inspection.
IVS-09.1: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?*	Y			Azure employs a defense in depth strategy for boundary protection, including secure segmentation of network environments through several methods including VLAN segmentation, ACL restrictions and encrypted communications for remote connectivity.
IVS-09.2: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?*	Y			Yes. System and network environments are isolated from each other using multiple technical controls.

IVS-09.3: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?*	Y			For the Azure infrastructure, production and non-production are physically and logically separated. Microsoft Azure employs network-based and host-based boundary protection devices such as firewalls, load balancers, IPFilters, jumpboxes and front-end components. These devices use mechanisms such as VLAN isolation, NAT and packet filtering to separate customer traffic from management traffic.
IVS-09.4: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?*	Y			Logical segregation is implemented to restrict unauthorized customer access to files / directories of other customers.
IVS-10.1: Infrastructure & Virtualization Security - VM Security	*Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?*	Yes			Communication channels are logically or physically isolated from other networks. Customer information is encrypted during transmission over external networks. Customer configuration information (e.g. connection strings, application settings) supplied through the management portal is protected while in transit and at rest.
IVS-10.2: Infrastructure & Virtualization Security - VM Security	*Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?*			N/A	Microsoft does not provide physical server migration.
IVS-11.1: Infrastructure & Virtualization Security - Hypervisor Hardening	*Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and*	Y			Microsoft Azure enforces the concept of least privilege and restricts access to information systems including the hypervisor or hypervisor management plane using role based security groups. All management access requires multi-factor authentication, and all access is logged.

	supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?				
IVS-12.1: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?*	Y			Azure does not permit or allow wireless connections in the Azure network environment. Azure regularly scans for rogue wireless signals on a quarterly basis and rogue signals are investigated and removed.
IVS-12.2: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)*			N/A	Wireless access to the Azure Production environment is not permitted. Wireless connections to Microsoft's corporate network must follow MSIT requirements for system health, security configuration, and policy enforcement.
IVS-12.3: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized*	Y			Privileges to MCIO systems and network devices are assigned to personnel based on least privilege principles in accordance with job responsibilities. Access to privileges is restricted through security groups.

	(rogue) network devices for a timely disconnect from the network?				
IVS-13.1: Infrastructure & Virtualization Security - Network Architecture	*Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?*	Y			Internal Azure diagrams clearly define boundaries and data flows between zones having different data classification, trust levels or compliance and regulatory requirements.
IVS-13.2: Infrastructure & Virtualization Security - Network Architecture	*Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?*	Y			Network filtering is implemented to prevent spoofed traffic and restrict incoming and outgoing traffic to trusted platform components. The Microsoft Azure network is segregated to separate customer traffic from management traffic. In addition, the SQL Azure services layer includes TDS gateways that control information flows through stateful inspection. Microsoft Azure has implemented load balancers and traffic filters to control the flow of external traffic to Microsoft Azure components. Additionally, Microsoft Azure has established automated controls to monitor and detect internally initiated Denial of Service (DDoS) attacks.

Interoperability and Portability: Controls IPY-01 through IPY-05

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
IPY-01.1: Interoperability & Portability - APIs	*Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?*	Y			A full set of Windows PowerShell cmdlets for the Azure API Management API is available via the standard Azure PowerShell installer.
IPY-02.1: Interoperability & Portability - Data Request	*Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?*	Y			Azure customers maintain access to their unstructured data stored with Azure and is available upon demand.
IPY-03.1: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?*	Y			Microsoft Azure has established designated responsibilities to review and execute service specific agreements and security requirements with third party service providers. Exchange of information between Microsoft Azure and third parties is governed through Information Exchange Agreements.
IPY-03.2: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?*	Y			Azure policies and provisions provide for language-agnostic Microsoft Azure Storage Services REST APIs, Microsoft Azure Service Management REST APIs, AppFabric Service Bus REST APIs, AppFabric Access Control REST APIs using open, standard formats such as HTTP, XML, WRAP, and SWT along with an ecosystem of tools and libraries.
IPY-04.1: Interoperability & Portability - Standardized	*Can data import, data export and service management be conducted over secure (e.g., non-*	Y			Access to customer applications and data through the service management API requires authentication using the customer registered certificate over SSL. Access to a Storage Account is restricted through the designated Storage Account Key (SAK) or customer generated Shared Access Signature (SAS).

Network Protocols	*clear text and authenticated), industry accepted standardized network protocols?*				Access to media assets and content keys through the REST API requires authentication over SSL. Customer media assets are stored in customer specified storage accounts. Content keys and customer storage account credentials (i.e., SAK and SAS) are encrypted while at rest. Customer media is stored securely during content transformation and deleted upon completion of the requested transformation. Delivery of a media asset is based on customer defined access policy.
IPY-04.2: Interoperability & Portability - Standardized Network Protocols	*Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?*	Y			MCIO configures information systems to provide only essential capabilities and specifically prohibits or restricts the use of the functions, ports, protocols, and/or services as per GSA, NIST, CIS guidelines, or industry best practices.
IPY-05.1: Interoperability & Portability - Virtualization	*Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?*	Y			Microsoft Azure supports virtualization industry standards including the OVF format.
IPY-05.2: Interoperability & Portability - Virtualization	*Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?*	Y			All available custom hooks are documented

Mobile Security: Controls MOS-01 through MOS-20

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
MOS-01.1: Mobile Security - Anti-Malware	*Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-02.1: Mobile Security - Application Stores	*Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-03.1: Mobile Security - Approved Applications	*Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-04.1: Mobile Security - Approved Software for BYOD	*Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-05.1: Mobile Security - Awareness and Training	*Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-06.1: Mobile Security - Cloud Based Services	*Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-07.1: Mobile Security - Compatibility	*Do you have a documented application validation process for testing device, operating system and application compatibility issues?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-08.1: Mobile Security - Device Eligibility	*Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-09.1: Mobile Security - Device Inventory	*Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-10.1: Mobile Security - Device Management	*Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-11.1: Mobile Security - Encryption	*Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-12.1: Mobile Security - Jailbreaking and Rooting	*Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-12.2: Mobile Security - Jailbreaking and Rooting	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-13.1: Mobile Security - Legal	*Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-13.2: Mobile Security - Legal	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-14: Mobile Security - Lockout Screen	*Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-15: Mobile Security - Operating Systems	*Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-16.1: Mobile Security - Passwords	*Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?*			N / A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-16.2: Mobile Security - Passwords	*Are your password policies enforced through technical controls (i.e. MDM)?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-16.3: Mobile Security - Passwords	*Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.1: Mobile Security - Policy	*Do you have a policy that requires BYOD users to perform backups of specified corporate data?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.2: Mobile Security - Policy	*Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-17.3: Mobile Security - Policy	*Do you have a policy that requires BYOD users to use anti-malware software (where supported)?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-18.1: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-18.2: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

MOS-19.1: Mobile Security - Security Patches	*Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-19.2: Mobile Security - Security Patches	*Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-20.1: Mobile Security - Users	*Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.
MOS-20.2: Mobile Security - Users	*Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?*			N/A	Wireless / mobile access to Azure production networks is not permitted within the datacenters.

Security Incident Management, E-Discovery & Cloud Forensics: Controls SEF-01 through SEF-05

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
SEF-01.1: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance	*Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?*	Y			Microsoft Azure has designated responsibilities and established processes to maintain contacts with external authorities across all jurisdictions in which it operates. MCIO has established procedures to receive, generate and disseminate security alerts from external organizations as necessary. MCIO coordinates with external agencies regarding the implementing of security directives.
SEF-02.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you have a documented security incident response plan?*	Y			Microsoft Azure has developed robust processes to facilitate a coordinated response to incidents if one was to occur. A security event may include, among other things unauthorized access resulting in loss, disclosure or alteration of data. The Microsoft Azure Incident Response process follows the following phases: • **Identification** – System and security alerts may be harvested, correlated, and analyzed. Events are investigated by Microsoft operational and security organizations. If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft. This escalation will include product, security, and engineering specialists. • **Containment** – The escalation team evaluates the scope and impact of an incident. The immediate priority of the escalation team is to ensure the incident is contained and data is safe. The escalation team forms the response, performs appropriate testing, and implements changes. In the case where in-depth investigation is required, content is collected from the subject systems using best-of-breed forensic software and industry best practices. • **Eradication** – After the situation is contained, the escalation team moves toward eradicating any damage caused by the security breach, and identifies the root cause for why the security issue occurred. If vulnerability is determined, the escalation team reports the issue to product engineering. • **Recovery** – During recovery, software or configuration updates are applied to the system and services are returned to a full working capacity. • **Lessons Learned** – Each security incident is analyzed to ensure the appropriate mitigations applied to protect against future reoccurrence.

SEF-02.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you integrate customized tenant requirements into your security incident response plans?*	Y			In the event a tenant is impacted by an event, Azure has clearly defined incident response plans and notification requirements.
SEF-02.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?*	Y			Microsoft publishes information on Security Incident Notification as part of the Azure Online Services Terms available publicly here: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31. If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident. Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.
SEF-02.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Have you tested your security incident response plans in the last year?*	Y			Security and incident response plans are continually updated and tested at least annually.
SEF-03.1: Security Incident Management, E-Discovery & Cloud Forensics	*Does your security information and event management (SIEM) system merge data*	Y			Azure Diagnostics are extensions that enable you to collect diagnostic telemetry data from a worker role, web role, or virtual machine running in Azure. The telemetry data is stored in an Azure storage account and can be used for debugging and troubleshooting, measuring performance, monitoring

- Incident Reporting	*sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?*				resource usage, traffic analysis and capacity planning, and auditing.
SEF-03.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting	*Does your logging and monitoring framework allow isolation of an incident to specific tenants?*	Y			The Azure logging and monitoring infrastructure encompasses the entire Azure platform and does not vary by tenant. Detected incidents are isolated or contained in the most effective way depending on the nature of the event.
SEF-04.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?*	Y			Security incident response plans and collection of evidence adheres to the ISO 27001 standards. MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the TSG are followed.
SEF-04.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?*	Y			MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the TSG are followed.
SEF-04.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?*	Y			In the event a follow-up action concerning a person or organization after an information security incident requires legal action proper forensic procedures including chain of custody shall be required for preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, impacted customers (tenants) and/or other external business relationships of a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.
SEF-04.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?*	Y			MCIO has established processes for evidence collection and preservation for troubleshooting an incident and analyzing the root cause. In case a security incident involves legal action such as subpoena form, the guidelines described in the TSG are followed.

SEF-05.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Do you monitor and quantify the types, volumes and impacts on all information security incidents?*	Y			An incident management framework has been established and communicated with defined processes, roles and responsibilities for the detection, escalation and response of incidents. Incident management teams perform 24x7 monitoring, including documentation, classification, escalation and coordination of incidents per documented procedures.
SEF-05.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Will you share statistical information for security incident data with your tenants upon request?*	Y			Microsoft Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Microsoft Azure customers are updated on the Microsoft Azure website in a timely manner.

Supply Chain Management, Transparency and Accountability: Controls STA-01 through STA-09

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
STA-01.1: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?*	Y			Azure works with various business groups to protect against supply chain threats throughout the supply chain lifecycle. These groups support Azure in creating purchase orders, accelerating deliveries, performing quality checks, processing warranty claims and obtaining spares.
STA-01.2: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?*	Y			Third party vendors are required to comply with Microsoft security policies and are audited. The Hardware Supply Management (HSM) group works with the MCIO business groups to protect against supply chain threats throughout the supply chain lifecycle. HSM supports MCIO in creating purchase orders, accelerating deliveries, performing quality checks, processing warranty claims and obtaining spares.
STA-02.1: Supply Chain Management, Transparency and Accountability - Incident Reporting	*Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?*	Y			Microsoft Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Microsoft Azure customers are updated on the Microsoft Azure website in a timely manner.
STA-03.1: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Do you collect capacity and use data for all relevant components of your cloud service offering?*	Y			Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, our network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. Proactive monitoring continuously measures the performance of key subsystems of the Microsoft Azure services platform

					against the established boundaries for acceptable service performance and availability. When a threshold is reached or an irregular event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.
STA-03.2: Supply Chain Management, Transparency and Accountability - Network / Infrastructure Services	*Do you provide tenants with capacity planning and use reports?*	Y			Microsoft Azure Capacity Management team projects future capacity requirements based on internal operational reports, revenue forecasts and inputs from internal component teams. Customers may use the Azure Operational Insights dashboard to monitor and adjust their virtual environment according to their needs.
STA-04.1: Supply Chain Management, Transparency and Accountability - Provider Internal Assessments	*Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?*	Y			Microsoft Azure performs risk assessments of its environment to review the effectiveness of information security controls and safeguards, as well as to identify new risks. The risks are assessed annually and the results of the risk assessment are presented to the management through a formal risk assessment report. Supplier scorecards have been developed to allow comparison and visibly monitor the performance of our suppliers using a balanced scorecard approach.
STA-05.1: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?*	Y			Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging third party services. The engaging team within Microsoft Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications.
STA-05.2: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?*	Y			Microsoft requires that vendors comply with applicable laws, including data protection laws. Vendors must also sign on to Microsoft's EU Model Clauses, which requires compliance with EU data protection law.
STA-05.3: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Does legal counsel review all third-party agreements?*	Y			Microsoft requires all vendors to sign our agreements, which have had legal review; all third-party agreements involving access to customer data also go through legal review.

STA-05.4: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do third-party agreements include provision for the security and protection of information and assets?*	Y			Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated Microsoft Azure manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within Microsoft Azure is responsible for managing their third party relationships, including contract management, monitoring of metrics such as service level agreements, asset protection requirements and vendor access to relevant applications.
STA-05.5: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you provide the client with a list and copies of all sub-processing agreements and keep this updated?*	Y			Microsoft Azure provides a list of third party contractors on the Microsoft Trust Center: https://www.microsoft.com/en-us/TrustCenter/Privacy/default.aspx
STA-06.1: Supply Chain Management, Transparency and Accountability - Supply Chain Governance Reviews	*Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?*	Y			Security risks related to external parties, such as customers, contractors and vendors are identified and addressed through the following: 1. Customer risks are assessed in coordination with Microsoft CELA and appropriate customer agreements are established. 2. Third parties undergo a review process through Global Procurement and an approved vendor list has been established. Purchase orders to engage a third-party require an MMVA to be established or a review to be performed by CELA. Vendors requiring access to source code need to be approved by the GM and CELA, and sign a Source Code Licensing Agreement. 3. Additional risks related to granting access to facilities and information systems are controlled and managed by MSIT. Physical and network security for offsite vendor facilities are governed by MSIT.
STA-07.1: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?*	Y			Microsoft Azure has established procedures and designated responsibilities for managing changes to third-party services. Microsoft Azure's designated teams manage third-party relationship including contract management, monitoring metrics such as service-level agreements, and third party access to systems, in accordance with these procedures as well as corporate-wide third-party management processes.

STA-07.2: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?*	Y			Microsoft Azure has employed an independent assessor to develop a system assessment plan and conduct a controls assessment. Controls assessments are performed annually and the results are reported to relevant parties.
STA-07.3: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?*	Y			The services provided by third-party vendors are monitored against the service levels by designated responsibilities in Microsoft Azure, as defined in the Statement of Work (SOW). Procedures for monitoring breaches to contractual obligations and handling issues with vendors are established.
STA-07.4: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you review all agreements, policies and processes at least annually?*	Y			The services provided by third-party vendors are monitored against the service levels by designated responsibilities from Azure and contractually requires that its subcontractors meet important privacy and security requirements. Third party service providers are routinely audited by both Microsoft and independent audit teams.
STA-08.1: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Do you assure reasonable information security across your information supply chain by performing an annual review?*	Y			Microsoft Azure contractually requires that its subcontractors meet important privacy and security requirements. Requirements and contracts are reviewed at least annually or as renewed. Microsoft Azure AD performs quarterly ISMS reviews.
STA-08.2: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Does your annual review include all partners/third-party providers upon which your information supply chain depends?*	Y			Microsoft Azure has employed an independent assessor to develop a system assessment plan and conduct a controls assessment. Controls assessments are performed annually and the results are reported to relevant parties.
STA-09.1: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you permit tenants to perform independent vulnerability assessments?*	Y			For security and operational reasons, Microsoft Azure does not allow our customers to perform their own audits on Microsoft's Microsoft Azure platform service, although customers are allowed to perform non- invasive penetration testing of their own application with prior approval.

STA-09.2: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?*	Y			Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure platform at least quarterly. Attestation to scans and their remediation can be found in the compliance and audit report documentation on the Azure website.

Threat and Vulnerability Management: Controls TVM-01 through TVM-03

Control ID in CCM	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
TVM-01.1: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?*	Y			The Microsoft Azure Security group responds to malicious events, including escalating and engaging specialized support groups. A number of key security parameters are monitored to identify potentially malicious activity on the systems. When providing the Antimalware solution for Virtual Machines, Azure is responsible for ensuring the service is highly available, definitions are updated regularly, that configuration through the Azure Management Portal is effective and that the software detects and protects against all known types of malicious software. MCIO-managed hosts in the scope boundary are scanned to validate anti-virus clients are installed and current signature-definition files exist.
TVM-01.2: Threat and Vulnerability Management - Anti-Virus / Malicious Software	*Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?*	Y			Weekly and real-time scans are performed and alerts are generated to MOC upon detection of malicious code.
TVM-02.1: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Procedures have been established and implemented to scan for vulnerabilities on MCIO-managed hosts in the scope boundary. MCIO implements vulnerability scanning on server operating systems, databases, and network devices with appropriate vulnerability scanning tool. MCIO web applications are scanned with the appropriate scanning solution. The vulnerability scans are performed on a quarterly basis at minimum. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundary. Software updates are released through the monthly OS release cycle using change and release management procedures. Emergency out-of-band security software updates (0-day & Software Security Incident Response Process - SSIRP updates) are deployed as quickly as possible. If customers use the default "Auto Upgrade" option, software updates will be applied their VMs automatically. Otherwise, customers have the option to upgrade to the latest OS image through the portal. In

					case of a VM role, customers are responsible for evaluating and updating their VMs.
TVM-02.2: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Web applications are scanned with purpose-built, industry application security scanning tools.
TVM-02.3: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			Vulnerability scans are performed at least quarterly. Microsoft Azure contracts with independent assessors to perform penetration testing of the Microsoft Azure boundaries.
TVM-02.4: Threat and Vulnerability Management - Vulnerability / Patch Management	*Will you make the results of vulnerability scans available to tenants at their request?*		N		Azure does not provide scans of customer VMs or any customer applications running on the VMs. Patching customer VMs is the responsibility of customers.
TVM-02.5: Threat and Vulnerability Management - Vulnerability / Patch Management	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?*	Y			A formal change control process is in place for testing, authorizing and promoting source code builds from pre-production environments to production based on defined entry/exit check-lists for each pre-production gate.
TVM-02.6: Threat and Vulnerability Management - Vulnerability / Patch Management	*Will you provide your risk-based systems patching time frames to your tenants upon request?*	Y			Microsoft Azure maintains and notifies customers of potential changes and events that may impact security or availability of the services through an online Service Dashboard. Changes to the security commitments and security obligations of Microsoft Azure customers are updated on the Microsoft Azure website in a timely manner.
TVM-03.1: Threat and Vulnerability Management - Mobile Code	*Is mobile code authorized before its installation and use, and the code configuration checked, to ensure*	Y			The SDL policy documents the usage restrictions and implementation guidance on mobile technologies such as ActiveX, Flash, Silverlight and JavaScript. It also lists the outdated technologies that are not permitted in Microsoft Azure. The use of mobile code in the Microsoft Azure

	that the authorized mobile code operates according to a clearly defined security policy?				applications is reviewed during multiple phases of the SDL process.
TVM-03.2: Threat and Vulnerability Management - Mobile Code	*Is all unauthorized mobile code prevented from executing?*	Y			Multiple controls prevent unauthorized mobile code from executing.

2 References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, as well as specific items referenced in the main text:

- Microsoft Azure Home – general information and links about Microsoft Azure
    - http://azure.microsoft.com
- Microsoft Azure Developer Center – developer guidance and information
    - http://msdn.microsoft.com/en-us/azure/default.aspx
- Security Best Practices For Developing Microsoft Azure Applications (white paper)
    - http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx
- Microsoft's Security Development Lifecycle (SDL)
    - http://www.microsoft.com/security/sdl/
- Microsoft Cloud Infrastructure and Operations group
    - http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx
- Microsoft Security Response Center [where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported]
    - http://www.microsoft.com/security/msrc/default.aspx
    - Or via email to secure@microsoft.com.
- Service Trust Portal
    - https://www.microsoft.com/en-us/TrustCenter/STP/default.aspx

CAIQv3.0.1

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1 - Google Cloud (updated Jan 2017)

The information described in this paper is detailed as of the time of authorship. The information in this document does not amend or in any way alter Google's security obligations as part of its contractual agreement with Customer. Google may discontinue or change the processes, procedures and controls described in this document at any time without notice as we regularly innovate with new features and products within Google Cloud. Google's security obligations are described in its contractual agreement with Customer which may include our Data Processing Amendment and/or Data Processing and Security Terms if opted-in to by Customer.

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			Google uses a continuous build and release process informed by industry practices. The controls around code release are included in the scope of our SOC 2/3 report.
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.

		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			X	Google does not rely on software suppliers. All software is Google developed by Google and Google has a mature software development process.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes purpose built code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	X			Customers must agree to a Terms of Service and an Acceptable Use Policy prior to using Google Cloud Platform.
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	X			The customer must identify the appropriate trust levels for access to Google Cloud Platform and set sharing permissions accordingly. Customers are responsible for managing these types of features in their applications on Google Cloud Platform.

Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	X			The intent of this controls does not apply to Google Cloud Platform. However, Google conducts integrity checks on data written to its storage systems to ensure availability and replication.
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Google defines a data security architecture conducive to its operational needs and has demonstrated that this architecture satisfies industry standards such as FedRamp, NIST 800-53, SOC 2/3 and ISO 27001 security objectives.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	X			Google provides audits assertions using industry accepted formats such as ISAE 3402, SOC 2/3 and ISO 27001.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	X			Google makes its SOC 2/3 report and ISO 27001 certificate available to customers.

		AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	X			Google's security teams are committed to a strong perimeter and dedicated staff are responsible for the safety and security of Google's network infrastructure. Google conducts rigorous internal continuous testing of our network perimeter through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.
		AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Google conducts rigorous internal continuous testing of our application surface through various types of penetration exercises. In addition, Google coordinates external 3rd party penetration testing using qualified and certified penetration testers.
		AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	X			Google maintains an internal audit program consistent with indusdry best practices and regulatory requirements.
		AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	X			Google is committed to maintaining a program where independent verification of security, privacy and compliance controls are regularly reviewed. Google undergoes several independent third party audits to test for data safety, privacy, and security, as noted below: SOC 1 / 2 / 3 (Formerly SSAE16 or SAS 70) ISO 27001 ISO 27017 / 27018 PCI-DSS HIPAA
		AAC-02.6	Are the results of the penetration tests available to tenants at their request?		X		Google Security Policy prohibits sharing this information but customers may conduct their own testing on our products and services.
		AAC-02.7	Are the results of internal and external audits available to tenants at their request?	X			Google publishes and makes available its ISO 27001, 27017, 27018 and SOC3 reports online. Detailed information of some confidential reports can be obtained under NDA.

		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	X			The Google security team performs regular testing on systems and processes in addition to audits performed by Google's corporate Internal Audit team that cover multiple disciplines and operational aspects of Google.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer data is logically segregated by domain to allow data to be produced for a single tenant only. However, it is the responsibility of the customer to deal with legal requests. Google will provide customers with assistance with these requests, if necessary.
		AAC-03.2		Do you have capability to recover data for a specific customer in the case of a failure or data loss?	X			Google has built multiple redundancies in its systems to prevent permanent data loss. Data durability assurances are built in the the service specific terms as part of the the terms of service. https://cloud.google.com/terms/service-terms
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Customers can choose data location in US and Europe when configuring some their Google Cloud Platform services. If these selections are made around choice of data location this is backed by the service specific terms within Google's Terms of Service. https://cloud.google.com/terms/service-terms

		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			Google continuously surveys its compliance landscape and adjusts its policies and practices as needed. It is the customer's responsibility to configure the services, per Google best practices, to be in compliance with any requirements relevant to their operations or jurisdictions.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them	Do you provide tenants with geographically resilient hosting options?	X			Google operates a global network of data centers to reduce risks from geographical disruptions. The link below includes the locations of our data centers: http://www.google.com/about/datacenters/inside/locations/ Google does not depend on failover to other providers but builds redundancy and failover into its own global infrastructure. Google performs annual testing of its business continuity plans to simulate disaster scenarios that simulate catastrophic events that may disrupt Google operations.
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?		X		
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Google performs annual testing of its business continuity plans to simulate disaster scenarios that simulate catastrophic events that may disrupt Google operations.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from	Do you provide tenants with documentation showing the transport route of their data between your systems?		X		The Google datacenter network infrastructure is secured, monitored, and environmentally controlled. Due to the dynamic and sensitive nature of this information, Google does not share this information with tenants.

		BCR-03.2	unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Can tenants define how their data is transported and through which legal jurisdictions?		X		Customers can define the zone or region that data is available, but they may not define if it is transported through a given legal jurisdiction.
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			Engineering teams maintain procedures to facilitate the rapid reconstitution of services.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	X			Google anticipates physical threats to its datacenters and has implemented countermeasures to prevent or limit the impact from these threads. The video below provides an overview of our countermeasures: https://www.youtube.com/watch?v=cLory3qLoY8c'
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	X			Google carefully selects the locations of its datacenters to avoid exposure to high-impact environmental risk to the extent possible.

Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Essential hardware in Google data centers are hot swappable.
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	X			GCE (Google Compute Engine) provides the ability perform full or incremental snapshots (backups) of the entire hard disk, it can be restored later. Customers can also export / import an entire VM (Virtual Machine) image in the form of a tar archive. https://cloud.google.com/compute/docs/images https://cloud.google.com/compute/docs/disks/
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			Customers can export / import an entire VM image in the form of a tar archive. https://cloud.google.com/compute/docs/images
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			Customers can export / import an entire VM image in the form of a tar archive. https://cloud.google.com/compute/docs/images
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	X			GCE VM image exports/imports are OS / software independent.

Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and manmade threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			Google has implemented redundancies and safeguards in its datacenters to minimize the impact of service outages.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Google maintains a dashboard with service availability and service issues here: https://status.cloud.google.com/ https://www.google.com/appsstatus
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			Google provides customers with uptime availability metrics and industry standard audit reports and certifications.
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			Google maintains a dashboard with service availability and service issues here: https://status.cloud.google.com/ https://www.google.com/appsstatus
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Engineering teams maintain playbooks to facilitate the rapid reconstitution of services.

Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?	X			Customers need to manage this by leveraging the features of our storage services. Please see the product documentation for specifics: https://cloud.google.com/docs/storing-your-data
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	X			Customers are primarily responsible for legal requests. Google will assist customers where necessary. Google's process for handling law enforcement requests is detailed here: http://www.google.com/transparencyreport/userdatarequests/legalprocess/
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Google builds multiple redundancies in its systems to prevent permanent data loss. All files are replicated at least three times and to at least two data centers. However, Google provides IAAS storage capabilities - dealing with business specific requirements is the responsibility of the customer and the storage platform will support the customers requirements.
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	X			Google embeds redundancy as part of its architecture and failure is expected and corrected continuously. Google annually tests its disaster recovery program which simulates catastrophic events impacting engineering operations.
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			The authorization to provision additional processing capacity is obtained through budget approvals and managed through internal SLAs as part of an effective resource economy.

		CCC-01.2		Is documentation available that describes the installation, configuration and use of products/services/features?	X			https://cloud.google.com/docs/ https://gsuite.google.com/learning-center/
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Google follows a structured code development and release process. As part of this process code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	Google does not outsource the development of its code.
Change Control & Configuration *Management Quality Testing*	CCC-03	CCC-03.1	Organization shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?	X			Google provides high-level information on our tools and techniques in our SOC report and security whitepaper. Google performs quality reviews on its code as part of our standard continuous build and release process. Google performs at least annual reviews of our data centers to ensure our physical infrastructure operating procedures are implemented and followed. For customer deployments, our resellers/integration partners take the lead on ensuring that the deployment meets the customer requirements. Our deployment teams provide technical support to troubleshoot issues.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	X			Google maintains a dashboard with service availability and service issues here: https://status.cloud.google.com/ https://www.google.com/appsstatus Google maintains internal bug tracking of known product defects. Each bug is assigned a priority and severity rating based on the number of customers impacted and the level of potential exposure of customer data. Bugs are actioned based on those ratings and remediation actions are captured in the bug tickets.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			If a legitimate vulnerability requiring remediation has been identified by Google, it is logged, prioritized according to severity, and assigned an owner. Google tracks such issues and follows up frequently until they can verify that they have been remediated. We also have a Vulnerability Rewards Program to solicit external reports in problems in our services. Please see: http://www.google.com/about/appsecurity/reward-program/

		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			Google follows a structured code development and release process. As part of this process, all code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			Google uses automated configuration management tools, software release tools and mobile device management software to restrict and monitor the installation of unauthorized software.
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	X			Google's native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	X			Google Cloud Compute resources support tagging. Customers assign tags to help easily apply networking or firewall settings. Tags are used by networks and firewalls to identify which instances that certain firewall rules apply to. For example, if there are several instances that perform the same task, such as serving a large website, you can tag these instances with a shared word or term and then use that tag to give HTTP access to those instances. Tags are also reflected in the metadata server, so you can use them for applications running on your instances. https://cloud.google.com/compute/docs/label-or-tag-resources

		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata /hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	Google tags physical hardware. Components are inventoried for easy identification and tracking within Google facilities. Other hardware characteristics such as MAC are also used for identification.
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?	X			Google allows domain administrators to configure alerts for potential suspicious logins. Geographic location is one factor that could indicate a suspicious login.
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant’s data upon request?	X			Google may store customer data is the following locations: http://www.google.com/about/datacenters/inside/locations/
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	X			Google may store customer data is the following locations: http://www.google.com/about/datacenters/inside/locations/
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	X			Customers can apply their own data-labeling standard to information stored in Google Cloud Platform.
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	X			Many Cloud Platform Products allow customers to choose their geographic location, this setting is configured when the service is first set up and is covered by the service specific terms https://cloud.google.com/terms/service-terms

Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			Netflow policies are enforced through switch and router based ACLs. Network traffic dashboard and automated inventory tools provide real-time information on traffic flow enforcement.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	X			Data stored at rest can be configured to stay in a geographic region. This is determined at time of service set up and in covered by the service specific terms: https://cloud.google.com/terms/service-terms
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Google supports the use of open encryption methodologies. Google forces SSL for all authentication traffic. Customer data is encrypted when on Google's internal networks, at rest in Cloud storage, Cloud SQL database tables, and backups.
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Google uses encryption when customer data traverses public networks. Encryption may be open-source based or proprietary.

Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	X			Google maintain policies and procedures on data access and labelling
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	X			Google has established procedures and technical controls to help ensure production data remains in the secure boundary of the production network.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	X			Google's terms of service address data ownership and its internal data security policies govern data stewardship.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	X			Google supports secures deletion but the method and timing is not at the discretion of the tenant.

		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?		X		Google's process for data deletion upon termination is described in our Terms: For Google Cloud Platform https://cloud.google.com/terms/data-processing-terms For GSuite https://gsuite.google.com/intl/en_nz/terms/2013/1/premier_terms.html
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	X			Google maintains assets inventories and assigns ownership for managing its critical resources.
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	X			Google maintains a list of Sub-Processors: https://www.google.com/intx/en/work/apps/terms/subprocessors.html
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	X			Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week.

Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			Google uses certificates and ACLs to achieve authentication integrity.
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	X			Google provides customers with security documentation including a security whitepaper and SOC 2/3 report that describe how we operate a global network with replication, failover and offsite backups. For GCP users, the locality of data is for the most part customer controlled and is described here: https://cloud.google.com/docs/geography-and-regions
Datacenter Security *Offsite equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?		X		Google has strict policies and procedures to govern the management of the equipment lifecycle within its production data centers. Any disk that did, at any point in its lifecycle, contain customer data is subject to a series of data destruction processes before leaving Google's premises, and would need to be authorized by appropriate operations manager before release.
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	X			Google maintains a physical security policy that describes the requirements for maintaining a safe and secure work environment.

		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	X			Google trains its employees and contractors annually in its security policies. Third-parties agree to observe Google's security policies as part of their contract.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	X			Customers can choose data location when they initiate project set up. This is covered by our service specific terms: https://cloud.google.com/terms/service-terms
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Google Data centers maintain secure external perimeter protections. All data centers employ electronic card key access control system that are linked to a system alarm. Access to perimeter doors, shipping and receiving, and other critical areas is logged, including unauthorized activity. Failed access attempts are logged by the access control system and investigated as appropriate. Authorized access throughout the business operations and data centers is restricted based on an individual's job responsibilities. The fire doors at the data centers are alarmed and can only be opened from the inside. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to help cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. Security operations personnel manage the CCTV monitoring, recording and control equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. .
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	X			Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	X			Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	X			Google's use and management of encryption keys is transparent to customers. Encryption keys may be applied to a customer, a file, disk, or transaction level depending on the type of encryption employed.
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?	X			Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API.
		EKM-02.3		Do you maintain key management procedures?	X			Google maintains documentation on its key management process.
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Google maintains documentation on its key management process and provides controls to manage encryption keys through their lifecycle and protect against unauthorized use.
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X		Google uses a combination of open source and proprietary code to develop its encryption solutions
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			We encrypt data at rest in Google Cloud Platform.
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			Network packets are encrypted when they leave Google Compute Engine Instances.

		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?	X			Google has a service (currently in Beta) which allows customers to supply their own encryption keys via API.
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	X			Google maintains internal documentation for the use of its internal proprietary key management service.
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			Google uses a combination of open source and proprietary encryption formats and algorithms validated by Google security engineers.
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Google maintains its own encryption keys.
		EKM-04.3		Do you store encryption keys in the cloud?	X			Google stores its keys in its own production environment.
		EKM-04.4		Do you have separate key management and key usage duties?	X			Google's key management operates as a service for engineering teams to use in their application code.

Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			Google maintains security configurations for its machines and networking devices. The configurations are maintained and serve as master copies for comparison against production instances. Deviations are identified and corrected.
		GRM-01.2		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			Google has automated mechanisms to detect deviations from the desired security configuration of its infrastructure.
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	X			Google allows customers to use their own virtual image to use in Google Cloud platform. https://cloud.google.com/compute/docs/tutorials/building-images
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	X			Google Cloud platform provides the ability to log and monitor security and system health. https://cloud.google.com/docs/

		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Google performs risk assessments as required by ISO 27001.
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			At Google, managers are responsible for ensuring their direct reports complete the required trainings and affidavits.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	X			Google provides tenants with its security whitepaper and security FAQ that describes our security program. We also maintain our internal ISMS documentation required by ISO 27001.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) least once a year?	X			Google reviews its ISMS documentation annually as required by ISO 27001.

Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	X			Google maintains a robust vendor management program. Vendors who work with Google are required to comply with all relevant information security and privacy policies. In addition, Google has open-sourced its vendor management questionnaires for use by the community: https://opensource.googleblog.com/2016/03/scalable-vendor-security-reviews.html
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	X			Google's security and privacy policies align with ISO 27001.
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	X			Google agrees contractually with providers on adherence to Google's security and privacy policies and has a vendor audit program to determine compliance.
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	X			Google has mapped its security controls to the requirements of SOC 2/3, NIST 800-53 Rev. 3 and ISO27002
		GRM-06.4		Do you disclose which controls, standards, certifications and/or regulations you comply with?	X			Google commits to maintaining PCI, FedRAMP, SOC 2/3 audit report and ISO 27001 certification.
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Google maintains a personnel policy that includes disciplinary procedures.

		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			Google makes its internal policies available to all personnel. Communication of policies occurs via required training, and through ongoing e-mail and internal communication. Employees must review and confirm understanding of key security and privacy policies (including what actions are taken if an employee is in violation of said policy) at least annually, and records of certification are retained to ensure compliance. Google's code of conduct is available publically at our investor website: https://investor.google.com/corporate/code-of-conduct.html
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	X			Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	X			Google notifies tenants of material changes to our privacy policy. Our security policies are internal facing and we don't notify customer for changes.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	X			Google reviews its security policies at least annually. Google's cross functional security policy team meets periodically throughout the year to address emerging issues and risk and issue new or amend existing policies or guidelines, as needed.

Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			Google performs risk assessments as required by ISO 27001.
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	X			Google performs risk assessments as required by ISO 27001.
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	X			Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification.
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	X			Google has documented its risk management procedures as part of its ISMS that underlies our ISO 27001 certification. Documentation is made available to all individuals that may participate in or need to be informed of risk management and assessment programs.

Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	X			Google's security incident response process includes involvement of our privacy team. Customers are notified when an events impacts their data.
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	X			Google's privacy policy is informed by industry standards and tailored to Google's unique operation environment.
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	X			Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually.
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	X			Personnel are required to acknowledge the training they have completed.
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	X			Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google’s confidentiality and privacy policies.

		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			Completion of the training is required by our personnel policies.
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	X			Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually.
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	X			Google maintains personnel and data access policies that govern the administration of access controls including transfers and terminations.
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			Google's personnel policies including considerations for the timely removal of access and return to Google issued assets.

Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e. g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			Google maintains a mobile device policy that details our requirements for mobile device use at Google. Customer data is not permitted on mobile devices.
Human Resources *Nondisclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	X			Google reviews NDA and confidentiality documents as needed.

Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			Google's Terms of Service outline the responsibilities of Google and customers.
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may or access tenant data and metadata?	X			Google maintains a Data Security policy that governs our access policies. All access to production resources require 2-factor authentication. Our Data Processing Amendment details on security measures including access controls: https://cloud.google.com/terms/data-processing-terms
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?		X		Our Data Processing Amendment details how we process tenant data. https://cloud.google.com/terms/data-processing-terms https://gsuite.google.com/terms/dpa_terms.html
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			X	Our Data Processing Amendment details how we process tenant data. https://cloud.google.com/terms/data-processing-terms https://gsuite.google.com/terms/dpa_terms.html

Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	X			Google provides Google-specific security training. The training is administered online and completion tracked. Completion is required annually.
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			This is primarily a customer responsibility as they own their data. Google personnel are trained on the Data Security policy including procedures for handling customer data.
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.

		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	X			Google maintains a security awareness program for its personnel. Customers are responsible for training their users.
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	X			*Google maintains a Data Security policy that governs conflict of interests.*
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	X			Google maintains a Data Security policy that governs access to data and mechanism to prevent and detect unauthorized access.
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	X			Google does not use a virtual infrastructure. Google maintains configuration management tools to detect and correct deviations from its security baselines and collects and secures audit records.
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	X			Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools.

		IAM-01.2		Do you monitor and log privileged access (administrator level) to information security management systems?	X			Google maintains automated log collection and analysis tools. Multi-factor authentication is required for any connections to our production environment.
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	Google makes its personnel policy available to all personnel and reminds employees as part of training and ongoing email communication action that may be a violation of its policies. Google's code of conduct is available publically at our investor website: https://investor.google.com/corporate/code-of-conduct.html	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			Google maintains an automated access revocation process that include account locking and revocation of certificates and role assignment.

		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	X			Google logs all changes in user permissions with the date and time of such changes.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	X			Google's production environment is segregated from our corporate environment.
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Google maintains a central identity and authorization management system.
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			Google maintains a central identity and authorization management system.

Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	X			Google provides (under a specific NDA) customers with a SOC 2/3 report that includes testing of Google's access controls. Details are documented here: https://cloud.google.com/security/whitepaper
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	X			Google follows a structured code development and release process. As part of this process, code is peer reviewed. Google makes proprietary code analysis tools available for engineers to deploy against application code. Google also performs continuous post-production tests based on real-time threats.
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	X			Google restricts access based on need-to-know and job functions. Google maintains automated log collection and analysis tools.
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	X			Google automatically replicates to and serves data from multiple data centers to provide seamless access to end-users should a datacenter not be available.
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	X			Google has designed redundancies in its system to help prevent service interruptions in the event of failure of in Google or a provider operated infrastructure.
		IAM-07.3		Do you have more than one provider for each service you depend on?	X			We have redundancy for critical services such as telecommunication links.

		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?		X		Google runs and maintains its own infrastructure and does not depend on external services. Due to both the dynamic and sensitive nature of this information, Google does not provide this information externally. However, macro service availability is visible below, and the regional coverage and guides on deploying highly available services is also available. https://status.cloud.google.com/ https://cloud.google.com/about/locations/ https://cloud.google.com/docs/geography-and-regions
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?		X		A tenant can contact support 24/7 to raise issues.
		IAM-07.6		Do you provided a tenant-triggered failover option?	X			Google Cloud platform provides a managed load balancing and failover capability to customers. https://cloud.google.com/compute/docs/load-balancing/
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?		X		Our business continuity program is verified as part of our SOC 2/3 audit report.
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	X			Google maintains a Data Security policy that governs access to customer data. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?			X	Not Applicable

Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			Customers are responsible for configuring the access by their uses to the service. For Google personnel, authorization is required prior to access being granted.
		IAM-09.2		Do your provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?			X	Customers are responsible for configuring the access by their users to the service. For Google personnel, authorization is required prior to access being granted.
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	X			Google requires access reviews at least annually for critical access groups.

		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	X			Google logs all changes in user permissions. Google revokes access when no longer required.
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?		X		Google notifies customers of security incidents that impact their data and will work with the customer in good faith to address any known breach of Google's security obligations.
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	X			Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access list and removes access that is no longer required. All account actions are recorded.
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			Google monitors its access lists carefully to minimize the potential for unauthorized account use. Google periodically reviews access lists and removes access that is no longer required. All account actions are recorded.

Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			Google supports integration with a customer's SSO solution: https://cloud.google.com/docs/permissions-overview https://support.google.com/a/answer/6087519 https://support.google.com/a/answer/60224?hl=en&ref_topic=6348126
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	X			Google support open standards such as OAuth, OpenID and SAML 2.0.
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating /authorizing users?	X			Google supports SAML as means for authenticating users.
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	X			Google Cloud Identity & Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. IAM access policies are defined at the project level using granular controls of users and groups or using ACLs. https://cloud.google.com/iam/ https://cloud.google.com/compute/docs/access/
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			Customers can integrate authentication to GSuite to their existing identity management system. Customers can customize access to data by organization and user and assign administrative access profiles based on roles.

		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	X			Google provides the capability for domain administrators to enforce Google's 2-step verification. The 2nd factor could be a code generated by Google's Authenticator mobile application or via a supported hardware key. Should a tenant choose to set up SSO against their own password management system, they would be able to leverage any 3rd party multifactor option that their system supports
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	X			Google supports integration with third-party identity assurance services.
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	X			Gsuite native authentication requires a minimum 8 character complex password. Tenants can set the maximum or increase the minimum. A built-in Password Monitor is visible to the end user upon password creation and to the System Administrators of the tenant whom can decide to force a password change on any user that is later detected to have a password that is weak. Google's native authentication has protections in place that would detect a brute force attack and challenge the user to solve a Captcha and would auto lock the account if suspicious activity is detected. The tenant's System Administrators can reset that account for the end user.
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			Custom policies can be enforced through SSO integration which is available as a standard part of our offering
		IAM-12.10		Do you support the ability to force password changes upon first logon?	X			Google by default requires a password change upon first login
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			Administrators can manually lock and unlock accounts.

Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	X			ACLs for production tools are appropriately scoped to perform job function.
		IAM-13.2		Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	X			Google continuously monitors our Cloud infrastructure.
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	X			The cloud platform infrastructure is appropriately hardened to minimize attack surface.
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	X			Google has implemented network and host based tools to detect and respond to potential security incidents. Google maintains automated log collection and analysis tools to support investigations.
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	X			Google restricts physical and logical access to audit logs.

		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	X			Google has mapped its security controls to the requirements of SOC 2/3, NIST 800-53 Rev. 3 and ISO27002.
		IVS-01.4		Are audit logs centrally stored and retained?	X			Google maintains an automated log collection and analysis tool to review and analyse log events.
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Google maintains an automated log collection and analysis tool to review and analyse log events.
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Google machine configuration changes are continuously monitored when online.
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?	X			Google Cloud platform provides the ability to log and monitor the health of virtual instances using variety of tools : https://console.developers.google.com https://cloud.google.com/docs/

Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			Google uses a synchronized time-service protocol to ensure all systems have a common time reference.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/ scenarios?			X	Google maintains an effective resource economy with internal SLAs between engineering teams that provide for capacity planning and provisioning decisions.
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	X			Google has implemented efficient memory management techniques in the virtual machine system.
		IVS-04.3		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	X			Google maintains an effective resource economy with internal SLAs between engineering teams that provide for capacity planning and provisioning decisions.

		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	X			Google's engineering teams monitor the performance and health of infrastructure components against their internal SLA commitments that in turn support business and regulatory requirements.
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	X			Google performs fuzz testing, penetration testing, and vulnerability scanning to detect, mitigate, and resolve security issues.
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	X			cloud.google.com/docs
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones ?			X	Google maintains these diagrams for internal purposes, but due the dynamic and sensitive nature of the information, does not share it externally.

		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	X			The security state of network devices in monitored continuously.
		IVS-06.4		Are all firewall access control lists documented with business justification?	X			Network ACLs are documented within configuration files with comments on purpose, as appropriate.
Infrastructure & Virtualization Security OS Hardening and Bass Controls	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	X			Google builds in own machines and deploys custom operating system images that only permit the necessary ports, protocols and services.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Customers can provision separate domains or organizations with a domain for testing purposes.
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	X			Google provides solution papers and reference Development and Test environments. https://cloud.google.com/solutions/devtest/

		IVS-08.3		Google Cloud platform provides the ability to log and monitor the health of virtual instances using a variety of tools : https://console.developers.google.com https://cloud.google.com/docs/	X			Google segregates its production environment from its corporate environment.
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Google employs multiple layers of network devices to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate defensive controls in its perimeter and boundaries.
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	X			Google employs multiple layers of network devices to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate defensive controls in its perimeter and boundaries.
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	X			Google segregates its production and corporate environments with appropriate network boundary controls.

		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			Google treats all user data as sensitive and applies the same network boundary controls. Customers can use organizational structures with their environment to help manage segregation of sensitive data.
Infrastructure & Virtualization Security *VM Security - Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	X			Traffic on Google's networks is encrypted.
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	X			Google's production network is separated from other networks.

Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			All access to production systems are based on least privilege, requires two-factor authentication, and is logged.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X	Google does not permit wireless access in the production environment. Google has established policies and procedures to manage in corporate wireless network perimeter.

		IVS-12.2	network	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)			X	Google does not permit wireless access points in its production environment. Google has established strong encryption and authentication to its corporate wireless network.
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	X			Google does not permit wireless access points in its production environment and periodically scans for rogue devices.
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?			X	Google maintains one homogeneous operating environment for Google Cloud Platform

		IVS-13.2	denial-of-service (DDoS) attacks.	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google intrusion detection involves: 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures; 2. Employing intelligent detection controls at data entry points; and 3. Employing technologies that automatically remedy certain dangerous situations.
Interoperability & Portability *APIs*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Google publishes information on its Cloud Platform APIs here: https://cloud.google.com/docs/ API's for the SaaS service are all standard and published here: https://developers.google.com/admin-sdk/" API's for GSuite are published here: https://developers.google.com/google-apps/
Interoperability & Portability *Data Request*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Customers do not need Google's assistance to port their data. Customers can export their data from GSuite on-demand using Google Takeout Services, https://takeout.google.com/settings/takeout, or Google Vault export functions, or the Data API's located in the GSuite Admin SDK. Customers can export their Google Cloud Platform data in a number of industry standard formats.
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	X			Customers should evaluate the APIs Google provides for suitability in third-party applications. Google makes detailed information available on the use and function of its APIs.

		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			SLAs are covered by the service specific terms: https://cloud.google.com/terms/service-terms https://gsuite.google.com/terms/2013/1/premier_terms.html
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Network traffic is encrypted using industry standard protocols.
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	X			cloud.google.com/docs
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability?	X			Google is the industry leader in Containers: https://cloud.google.com/compute/docs/containers

		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	X			Google uses the KVM hypervisor. Security enhancements made to the KVM hypervisor are documented here: https://cloudplatform.googleblog.com/2017/01/7-ways-we-harden-our-KVM-hypervisor-at-Google-Cloud-security-in-plaintext.html
Mobile Security *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	X			Google provides security awareness training to all employees that include reference to our security policies. Our security policies include our mobile policy which specifies the security protection required to reduce the risk of, for instance, malware. Further mobile devices are prohibited from accessing production networks.
Mobile Security *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	X			Google's mobile device policy does not permit the use of third-party application stores.
Mobile Security *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	X			The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a Work Profile is required which includes a restricted Apps Store.

Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X	The Google Device Policy restricts the user and device behavior on mobile devices including application installation. For advanced use, a Work Profile is required which includes a restricted Apps Store.
Mobile Security *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	X			Google provides security awareness training to all employees that include reference to our security policies which include our mobile policy.
Mobile Security *Cloud Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	X			Google only permits the storage of Google sensitive information in approved systems.
Mobile Security *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	X			Mobile operability is is part of our standard software engineering development lifecycle.
Mobile Security *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	X			Google maintains a mobile policy and provides detailed instructions to personnel that wish to provision access to Google services on their mobile device. The policy includes eligibility requirements and security policy requirements.

Mobile Security *Device Inventory*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	X			All devices must register through the Google Device Policy Manager unless browser-only access is used.
Mobile Security *Device Management*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	X			Google's Device Policy Manager enforces Google's mobile policy except when access is solely to Apps services and through a browser.
Mobile Security *Encryption*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	X			Mobile devices with access to corporate resources other than Apps services require encryption.
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	X			Google's mobile policy does not permit jailbreaking or rooting on devices linked to a Google corporate account.

		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	X			Google's Device Policy Manager may not install on a device that does not conform the the required security specifications. The Device Policy Manager is required in order to access corporate sources using mobile applications.
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	X			Google's mobile policy states that all security policies continue to apply.
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	X			Google's Device Policy Manager may not install on a device that does not conform the the required security specifications. The Device Policy Manager is required in order to access corporate sources using mobile applications.
Mobile Security *Lockout Screen*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	X			Google's Device Policy Manager requires personnel to set an automatic lockout screen.

Mobile Security *Operating Systems*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	X			Google's Device Policy Manager requires personnel to keep devices up to date with patches and requires a minimum O/S level.
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	X			Google's Device Policy Manager enforces password policies.
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?	X			Google's Device Policy Manager enforces password policies.
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	X			User can choose their authentication setting as long as minimum requirements such as 4 point swipe pattern or PIN.
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X	Data from Google services are synced from the cloud data store to the device.
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	X			Google's mobile device policy does not permit the use of unapproved application stores.

		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	X			Google's mobile device policy but requires a device configuration and uses reduces the risk of malware from being installed on the device.
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	X			Google's supports remote wipe capabilities for mobile devices with access to sensitive corporate information.
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	X			Google's supports remote wipe capabilities for mobile devices with access to sensitive corporate information.
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	X			The management of O/S levels is the responsibility of the user. Google's mobile policy requires the installation of all updates and sets minimum O/S requirements.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	X			The management of O/S levels is the responsibility of the user. Google's mobile policy requires the installation of all updates and sets minimum O/S requirements.
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	X			Google's mobile policy defines which corporate resources can be accessed with a mobile device and the level of protections associated with such access.

		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	X			Google's mobile policy defines which roles (profiles) can access corporate resources.
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	X			Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	X			Google maintains incident response procedures to help ensure prompt notification and investigation of incidents.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		X		Google has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Due to the fact that the incident response system is standardized, customization of the notification process is not supported for each tenant.
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	X			The terms of service cover roles and responsibilities. https://cloud.google.com/terms/
		SEF-02.4		Have you tested your security incident response plans in the last year?	X			Google performs annual testing of its emergency response processes.

Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	X			Google maintains automated log collection and analysis tools that collect and correlate log information from various sources.
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	X			Google maintains automated log collection and analysis tools that support the investigation of incidents not caused by the tenant.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			Google can support valid request for specific tenant data from law enforcement.
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			Google can support valid request for specific tenant data from law enforcement.
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			For Cloud Platform: Customer would need to implement this feature on their own. Which is possible with GCP features and services. Gsuite provides the Apps Vault product which can be used by the customer for litigation holds.

		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Google can support valid request for specific tenant data from law enforcement.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	X			Google reviews and analyzes security incidents to determine impact, cause and opportunities for corrective action.
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		X		The amount of security incident data is currently statistically insignificantly small. Should the amount of data increase, Google will consider sharing this statistical information.
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?			X	Google does not depend on supply-chain partners for data quality with respect to delivering the Google Cloud Platform service.
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.

Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Individual customers get notified should an incident impact their data. Google communicates outage information through our status dashboards: For Cloud Platform: https://status.cloud.google.com/ For Gsuite: https://www.google.com/appsstatus#hl=en&v=status
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Google collects capacity and use data on its infrastructure as needed to information capacity planning and internal SLA performance.
		STA-03.2		Do you provide tenants with capacity planning and use reports?			X	Not applicable to GCP
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Engineering teams perform quarterly performance reviews and at least annually update SLAs and performance metrics.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	X			Subprocessor agreements are subject to all applicable laws and regulations.
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	X			Subprocessor agreements are subject to all applicable laws and regulations.

		STA-05.3	business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Does legal counsel review all third-party agreements?	X			Google's policy is that the Legal department reviews third-party contracts.
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?		X		Subprocessor information is available here: https://www.google.com/intx/en/work/apps/terms/subprocessors.html

Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	X			The customer terms of services are updated as needed.
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.

		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	X			Internal reviews of supplier contracts may consider conflicts of interest, as applicable, based on the nature of the contract.
		STA-07.4		Do you review all agreements, policies and processes at least annually?	X			Relevant policies and processes are reviewed annually.
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
		STA-8.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	X			Google employs a vendor management process that includes contractual requirements to adhere to Google's security policies and onsite inspections, as needed, to confirm compliance.
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?	X			Google permits customers to conduct their own vulnerability scans and penetration tests. In addition, Google maintains a robust bug bounty program and encourages input from the security community. For details see: http://www.google.com/about/appsecurity/reward-program/
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			Google retains a 3rd party to conduct periodic penetration tests.

Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?			X	Malware detection is included in our GSuite service. GMail scans for malware in email and attachments and Drive scans files prior to upload.
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	X			Google's threat detection systems are constantly updated based on attack signatures encountered.
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic network vulnerability scans using commercial tools.
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic application-layer vulnerability scans using commercial and proprietary tools.
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			Google performs periodic local operating system-layer scans and checks using commercial and proprietary tools.
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?		X		Google does not make vulnerability scan results available to customers but customers can perform their own scans. Google files bug tickets for any identified issues that require remediation. Bug tickets are assigned a priority rating and are monitor for resolution.

		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	X			Google operates a homogeneous machine environment with custom software to minimize exposure to vulnerabilities in commercial products and to allow rapid patching if needed.
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?		X		Google currently patches systems as needed and as quickly as vulnerabilities are addressed rather than on a scheduled basis. The notification process is determined in the terms of service and security guides. https://cloud.google.com/security/whitepaper https://cloud.google.com/terms/
Threat and Vulnerability Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?			X	Google Cloud Platform does not rely on mobile code.
		TVM-03.2		Is all unauthorized mobile code prevented from executing?			X	Google Cloud Platform does not rely on mobile code.
© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ Version 3.0.1" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 (2014). If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.								

IBM Cloud platform

V2 June 2018

Introduction

Designed using secure engineering practices, the IBM Cloud platform has layered security controls across network and infrastructure. It aligns with a broader set of IBM security and privacy standards which are referenced where applicable in this CSA CAIQ submission. IBM Cloud platform ensures security readiness by adhering to security policies that are driven by best practices in IBM for systems, networking, and secure engineering. These policies include practices such as source code scanning, dynamic scanning, threat modelling, and penetration testing. In addition, IBM Cloud platform provides a group of security services that can be used by application developers to secure their mobile and web apps. These elements combine to make IBM Cloud a platform with clear choices for secure application development.

IBM Cloud platform Public and Dedicated use IBM Cloud infrastructure services and take full advantage of its security architecture. IBM Cloud infrastructure provides multiple, overlapping tiers of protection for your applications and data. In addition, IBM Cloud platform adds security capabilities at the Platform as a Service layer in different categories: platform, data, and application.

IBM Cloud platform has been assessed by independent auditors as part of many compliance standard certifications including ISO 27001 and SOC2. Refer to this link for more details on the different compliance standards applicable to IBM Cloud platform
https://console.bluemix.net/docs/security/compliance.html#compliance

For more reading on how IBM security and privacy standards ensure complete privacy and security for our customer data, refer to these links
https://www.ibm.com/security/secure-engineering/
https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy

For IBM Cloud platform, refer to these links for additional information on using it to develop and deploy secure applications and services with IBM Cloud Foundry and IBM Cloud Container Service.
https://console.bluemix.net/docs/security/index.html#security
https://console.bluemix.net/docs/containers/cs_secure.html - security
https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/

The CAIQ was designed to help with one of the leading concerns that companies have when moving to the cloud: the lack of transparency into what technologies and tactics cloud providers implement, relative to data protection and risk management, and how they implement them. This CAIQ document gives detailed responses to those questions for the IBM Cloud platform and provides additional links where required on IBM and IBM Cloud platform security processes.

Control Group	CID	Consensus Assessment Questions	IBM Response
Application & Interface Security *Application Security*	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	The IBM Secure Engineering Standard ensure security as part of our SDLC. Those standards include processes for secure coding, vulnerability assessment, penetration testing, education, processes for 3rd party code approval and threat modelling. The standards used are regularly evaluated and updated for inclusion or replacement. See https://www.ibm.com/security/ Penetration testing is performed by both IBM and third parties and covers both external and internal testing of endpoints. Vulnerability assessment requires automated code and application scanning in addition to manual testing. Secure coding mandates manual review for secure related code and reviews against OWASP top ten attacks. Blumemix has been certified by an independent auditor against the ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, manual code reviews, and other techniques.
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, manual code reviews, and other techniques.
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Development work for the IBM Cloud platform is not outsourced. For all 3rd party components used, e.g. libraries or open source code, the IBM Secure Engineering Standard prohibits their use unless approved by IBM's Open Source Software Process. That approval process includes technical, legal and marketing reviews.
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	The IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include automated static and dynamic scans, manual penetration tests, threat modeling, manual code reviews, and other techniques. New functionality or code may not be moved to production without a threat model and vulnerability assessment being performed.
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	IBM Cloud customers are ultimately responsible for the data integrity of their workload. IBM Cloud compliance certifications demonstrate the controls Cloud has in place to provide a secure platform. https://console.bluemix.net/docs/security/compliance.html#compliance
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	Requirements and trust levels for customer access are established contractually for each Customer.
Application & Interface Security *Data Integrity*	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. SOC2 compliance demonstrates the controls IBM Cloud platform has in place to safeguard against the unauthorized access, destruction, loss or alteration of data stored in Cloud platform.

Control Group	CID	Consensus Assessment Questions	IBM Response
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	All IBM Cloud platform data is encrypted in transit. Data in transit encryption uses TLS from internet to the reverse proxy at edge of IBM Cloud platform network which terminates TLS. For CF, IPSEC based encryption is provided within the IBM Cloud platform network for all data in transit from the reverse proxy to IBM Cloud platform components. IBM Cloud platform customers must ensure their applications are TLS enabled. Custom certs can be associated with the IBM Cloud platform endpoints as outlined here for Cloud Foundry and Container Service respectively. https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemix-custom-domains/ Need link for containers service. Data at rest encryption for a IBM Cloud platform application's data is the responsibility of the application developer, and they can use services provided by IBM Cloud - see details under the IBM Cloud Data Services section of the IBM Cloud catalog.
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	IBM Cloud platform uses external auditors to conduct multiple structured, industry standard audit assertions and reports. See https://console.bluemix.net/docs/security/compliance.html#compliance
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	IBM Cloud platform provides relevant third party audit certification reports where a Non Disclosure Agreement (NDA) is in place.
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Penetration testing is performed by IBM teams against IBM Cloud platform staging environments on at least a quarterly basis. This testing covers network and application level testing and includes testing for both SANS top25 and OWASP top ten vulnerabilities. 3rd-party vendors (external) perform application and network penetration against IBM Cloud platform Pen Test production environments (public and private clouds) on an annual basis. Those tests include both external testing against public endpoints and internal testing where the vendor is provided with access to the environment to test for any internal network vulnerabilities or weaknesses. For Public IBM Cloud platform, we can make available SOC2 report forlients who are under IBM NDA as we need to show evidence of penetration testing and vulnerability scanning to SOC2 auditor. For Dedicated IBM Cloud platform clients, we can make available penetration test and vulnerability scan reports "on request" to clients for their own Dedicated IBM Cloud platform environments on approval by IBM CISO.
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	

Control Group	CID	Consensus Assessment Questions	IBM Response
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Internal audits are conducted on at least an annual basis.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	IBM Cloud platform uses external auditors to conduct multiple structured, industry standard audit assertions and reports. See https://console.bluemix.net/docs/security/compliance.html#compliance
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	For Public IBM Cloud platform, which is multi-tenant, we can make available SOC2 report for clients who are under IBM NDA as we need to show evidence of penetration testing and vulnerability scanning to SOC2 auditor. For Dedicated IBM Cloud platform clients, we can make available penetration test and vulnerability scan reports "on request" to clients for their own Dedicated IBM Cloud platform environments on approval by IBM CISO.
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	IBM Cloud platform provides relevant third party audit certification reports where a Non Disclosure Agreement (NDA) is in place. Internal audit report releases must be approved by the IBM Office of the CIO.
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	IBM Cloud platform uses multiple internal entities to conduct cross functional audit assessments.
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	IBM Cloud Customers are responsible for the encryption of their data at rest but IBM Cloud Data services provides a number of options to encrypt that data. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/data/ Disk Partitions where customer data resides are encrypted using LUKS. IBM Container Service provides unique TLS certificates for default domains assigned for each cluster.
	AAC-03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. IBM Cloud Data services provide guidance on how to backup and recover data. Refer to the specific IBM Cloud Data Service within the IBM Cloud platform online documentation. https://console.bluemix.net/docs/services/WorkWithData/index.html#index Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups are encrypted and stored into IBM Cloud infrastructure Evault.

Control Group	CID	Consensus Assessment Questions	IBM Response
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	IBM Cloud provides customers with options to deploy their applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html
	AAC-03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	The IBM Cloud platform management team regularly surveys changes in the regulatory environment. The IBM Legal Department also monitors regulatory requirements for their impact upon IBM security programs. Customers are responsible for tracking any changes to their regulatory requirements.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	IBM Cloud platform provides a number of options to allow customers to deploy applications for high availability including high availability zones within a region and high availability across regions. There are a number of tutorials available at IBM developerworks and IBM Garage to assist the customer with their configurations, e.g. https://www.ibm.com/developerworks/cloud/library/cl-high-availability-and-disaster-recovery-in-bluemix-trs/index.html
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	IBM Cloud platform provides a number of options to allow customers to deploy applications with high availability and disaster recovery across regions.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Business continuity plans are regularly tested at least on an annual basis. The related controls have been verified by an external auditor as part of IBM Cloud platform is27001 certification.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	IBM Cloud platform provides customers the options to deploy their applications and data in different regions. The data remains in that region unless the customer moves it. Customers have different options on how they connect to their IBM Cloud platform dedicated instance, e.g. over public network or over a dedicated VPN from their enterprise Data transport diagrams for Dedicated environments are available to tenants.
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	Data transport can be defined up to a point but in the event of network connection failure alternate paths can be used though not specific to legal jurisdiction. Customers should take legal jurisdictions into account when designing and deploying their systems across multiple datacenters.
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information on securing applications in IBM Cloud platform is readily available in IBM Cloud platform docs, https://console.bluemix.net/docs/security/index.html#security, and through various online tutorials in IBM Developerworks and IBM Cloud Garage. For the Container service, see this link for information on configuring, installing, securing and operating kubernetes clusters: https://console.bluemix.net/docs/containers/container_index.html Information system documents that do not impact the security or availability of other tenants are available for Dedicated environments. Some information systems documents are restricted from release approval from the IBM CIO office.

Control Group	CID	Consensus Assessment Questions	IBM Response
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Physical and Environmental Protection controls are in place in all IBM data centers and are validated frequently through internal audits and by external auditors as part of NIST and iso27001 compliance NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Physical and Environmental Protection controls are in place in all IBM data centers and are validated frequently through internal audits and by external auditors as part of NIST and iso27001 compliance NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	IBM Cloud foundry runtimes does not include Virtual Infrastructure. IBM Container Service provisions virtual infrastructure in IBM Cloud infrastructure. Hardware restore and recovery is not applicable.
	BCR-07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	IBM Cloud foundry runtimes does not include Virtual Infrastructure. IBM Container Service provisions virtual infrastructure in IBM Cloud infrastructure and does not provide any time based virtual system restore options.
	BCR-07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	IBM Cloud Container Service only supports IBM Cloud infrastructure
	BCR-07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	IBM Cloud Container Service only supports IBM Cloud infrastructure
	BCR-07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	IBM Cloud Container Service only supports IBM Cloud infrastructure
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Physical and Environmental Protection controls are in place in all IBM data centers. These controls are maintained through frequent internal audits and are validated by external auditors through assessments such as FedRAMP, ISO27001 and SOC2. In addition, IBM Cloud platform provides a number of options to allow customers to deploy applications for high availability including high availability zones within a region and high availability across regions.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	IBM Cloud platform provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net
	BCR-09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	IBM Cloud platform provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net
	BCR-09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	IBM Cloud platform provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status and https://status.ng.bluemix.net

Control Group	CID	Consensus Assessment Questions	IBM Response
Business Continuity Management & Operational Resilience *Policy*	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	IBM Cloud platform has a set of Security Policies in place which are aligned with IBM Core Security Practices covering Systems, Networking and Secure Engineering best practices. Security readiness focal points are assigned for each IBM Cloud platform component and service and are responsible to drive conformance to those security policies.. All IBM employees are required to take security related education.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11.1	Do you have technical control capabilities to enforce tenant data retention policies?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. Refer to the IBM Cloud platform online documentation for more details on IBM Cloud Data services. https://console.bluemix.net/docs/services/WorkWithData/index.html#index Data retention policies and procedures for IBM Cloud platform Metadata and logs are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups for IBM Cloud Foundry Runtimes are encrypted and stored into IBM Sotflayer Evault. Kubernetes Cluster metadata backups are encrypted and stored into IBM Cloud Object storage. SOC2 compliance demonstrates the controls IBM Cloud platform has in place for data retention of IBM Cloud platform metadata and logs and to safeguard against the unauthorized access, destruction, loss or alteration of data stored in IBM Cloud platform.
	BCR-11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	IBM Cloud platform does not share customer data unless subject to disclosure to government agencies pursuant to judicial proceeding, court order, or legal process. For more details on privacy and trust, refer to https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy IBM complies with the U.S.-Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data from Switzerland. International Business Machines Corporation has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. To learn more about the Safe Harbor program, and to view IBM's certification, please visit http://www.export.gov/safeharbor/
	BCR-11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Data retention policies and procedures are defined and maintained in accordance to the applicable regulatory and compliance standard. Application Metadata backups for IBM Cloud Foundry Runtimes are encrypted and stored into IBM Sotflayer Evault. Kubernetes Cluster metadata backups are encrypted and stored into IBM Cloud Object storage.
	BCR-11.5	Do you test your backup or redundancy mechanisms at least annually?	Disaster recovery testing is conducted on at least an annual basis.

Control Group	CID	Consensus Assessment Questions	IBM Response
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	IBM Secure Engineering standard provides policies on the development, reviewing and scanning of code, applications and systems prior to deployment including any changes triggered via acquisition. All deployments are controlled via IBM Cloud platform Change Management Policy and associated procedures. https://www.ibm.com/security/secure-engineering/
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	Extensive documentation is available in the form of product documentation, white papers, tutorials and videos in IBM Cloud platform Docs and via IBM DeveloperWorks and IBM Cloud Garages sites. https://console.bluemix.net/docs/ https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/ https://www.ibm.com/cloud-computing/bluemix/garage https://console.bluemix.net/docs/containers/container_index.html#container_index https://www.ibm.com/cloud/garage/content/architecture/microservices/1_0
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	Development work for the IBM Cloud platform is not outsourced. For all 3rd party components used, e.g. libraries or open source code, the IBM Secure Engineering Standard prohibits their use unless approved by IBM's Open Source Software Process. That approval process includes technical, legal and marketing reviews.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	IBM Secure Engineering standard dictates multiple scanning techniques be used before the promotion of code into production. These include static and dynamic scans, penetration tests, threat modelling, manual code reviews, and other techniques. The CR process provides a high level of control for all software development activities. https://www.ibm.com/security/secure-engineering/
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	IBM Secure Engineering standard provides policies on the development, reviewing and scanning of code, applications and systems prior to deployment including any changes triggered via acquisition. The goal of the secure engineering standard is to assure quality and minimize risks to deployed systems. It enforces security education for all IBM staff with more specific security education based on role and mandates the use of threat modelling for all deployments which includes a risk assessment phase. https://www.ibm.com/security/secure-engineering/ IBM Cloud platform is iso27001 certified by external auditors. This certification is available to customers and has different control points which focus on quality assurance and risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html#compliance
	CCC-03.2	Is documentation describing known issues with certain products/services available?	IBM Cloud platform provides customers with visibility on status and maintenance notifications for all the platform and services via a number of public status pages. See https://console.bluemix.net/status

Control Group	CID	Consensus Assessment Questions	IBM Response
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	IBM Secure Engineering standard requires security validation tests and a security release checkpoint be completed before each release. https://www.ibm.com/security/secure-engineering/ IBM Product Security Incident Response Team (PSIRT) process is followed for security incident management (https://www.ibm.com/security/secure-engineering/process.html). The PSIRT team monitor and alert on any vulnerabilities discovered in any IBM system or software and each IBM Cloud platform and Service has assigned PSIRT Responders to act on those vulnerabilities. SLAs are in place to ensure timely assessment on whether each component is vulnerable and subsequent patching, with the SLAs varying depending on the CVSS score.
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	IBM Secure Engineering standard dictates that code reviews must be performed against a secure coding review checklist which includes checks to remove any debug code.
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	IBM Cloud platform has a Change Control process to manage and track changes to any portion of the system, regardless of its maturity level (Experimental, Beta or GA). The change control process requires multiple levels of review approval including component owners and management. For customer private clouds, the changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance. For Cloud Foundry, File integrity monitoring runs on all VMs in customer environments and tracks any unauthorized changes to that VM such as identity management, networking, system management and OS configuration. For the Container Service, If you have a standard cluster, you can use Kubernetes daemon sets for everything that you want to run on every worker node including File Integrity Monitoring
Change Control & Configuration Management *Production Changes*	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	IBM Cloud platform is SOC2 certified and this includes controls on change management. Reports can be made available to customers on request. For Public IBM Cloud, information about any changes that impact availability will be notified to customers. For dedicated and private environements, changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance.
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Dedicated virtual machines are assigned to customers in IBM Cloud platform dedicated environment. This information is readily available to IBM Cloud platform operations and utilizes real time inventory asset tracking.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	Dedicated hardware and virtual machines are assigned to each IBM Cloud platform dedicated customer. This information is readily available in the IBM Cloud infrastructure portal and can be shared with customers for their environment.
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	In dedicated IBM Cloud platform, customers can authenticate their own users via SSO and can utilize geography based authentication factors.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	IBM Cloud platform provides customers with options to deploy their containers, applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	IBM Cloud platform provides customers with options to deploy their containers, applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html A complete list of regions and datacenters is available at: https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	IBM Cloud platform customers are responsible for classifying their data

Control Group	CID	Consensus Assessment Questions	IBM Response
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	IBM Cloud platform provides customers with options to deploy their containers, applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html A complete list of regions and datacenters is available at: https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	IBM Cloud platform provides customers with options to deploy their containers, applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html A complete list of regions and datacenters is available at: https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations Access to customer data and application metadata may be required to provide customer support, troubleshoot the service, or comply with legal requirements. information about any potential access to that data from outside that region are documented and made available to customers.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Data in transit encryption uses TLS from internet to the reverse proxy at edge of IBM Cloud platform network which terminates TLS. IPSEC based encryption is provided within the IBM Cloud Foundry network from the reverse proxy to Cloud Foundry Router and from Cloud Foundry Router to the Cloud Foundry application container host in which the IBM Cloud platform application runs. All Container service control place communications are TLS encrypted. IBM Cloud platform customers must ensure their applications are TLS enabled. Custom certs can be associated with the IBM Cloud platform application endpoints as outlined here for Cloud Foundry and Container Service respectively: https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemix-custom-domains/ or using an API outlined here: http://bluemixapi-docs.stage1.mybluemix.net/swagger/?api=api-server#/default https://console.bluemix.net/docs/containers/cs_ingress.html#custom_domain_cert
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	IPSEC based encryption is utilized for all component to component traffic.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	IBM Cloud platform follows IBM Corporate Standards which dictate an extensive labeling and handling scheme for all assets containing IBM owned data. Containers with customer data are labeled and treated as such. IBM Cloud platform customers are responsible for managing and labelling their own data.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	IBM Cloud platform has segregated development, staging and production environments deployed in different VLANs in different IBM Cloud infrastructure accounts. Each customer environment is considered to be a production environment but IBM Cloud platform provides customer's with the ability to deploy code into production and non-production spaces. It is the customer's responsibility to restrict the movement of workload between their environments and ensure production data is not replicated to non-production environment. https://www.ibm.com/developerworks/cloud/library/cl-intro4-app/index.html

Control Group	CID	Consensus Assessment Questions	IBM Response
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	IBM Cloud platform follows IBM Corporate Standards which dictate an extensive labeling and handling scheme for all IBM owned data. Containers with customer data are labeled and treated as such. IBM Cloud platform customers are responsible for managing and labelling their own data.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	IBM employs a decommissioning and reclaim process for all hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. See http://blog.softlayer.com/tag/disposal
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	The process outlined in DSI07.1 is followed for any service being canceled in IBM Cloud platform.
Datacenter Security *Asset Management*	DCS-01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	IBM Cloud platform records all physical and virtual assets in a IBM asset inventory system that captures details including asset owner, classes of data managed, locations of hosting infrastructure and contact details. The asset inventory process has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance.
	DCS-01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	Critical suppliers are documented, along with appropriate contact information.
Datacenter Security *Controlled Access Points*	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	IBM Data centers are secured, with server-room access limited to certified employees. Physical security parameters can include but are not limited to fences, walls, barriers, security guards, gates, electronic surveillance, video surveillance, physical authentication mechanisms, reception desks, and security patrols. The controls have been certified by an external auditor. See NIST 800-53 PE and ISO27001 A11 for the relevant controls https://www.ibm.com/cloud-computing/bluemix/compliance See https://www.ibm.com/cloud-computing/bluemix/data-centers for more details on IBM Data center security.
Datacenter Security *Equipment Identification*	DCS-03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	IBM Cloud platform manages all assets following an IBM asset inventory process and this has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance
Datacenter Security *Offsite Authorization*	DCS-04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	IBM Cloud platform provides customers with options to deploy their containers, applications and data in different regions. That data is remains in that region unless the customer moves it. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html A complete list of regions and datacenters is available at: https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations
Datacenter Security *Offsite equipment*	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	IBM employs a decommissioning and reclaim process for all hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. See http://blog.softlayer.com/tag/disposal IBM Cloud platform manages all assets following an IBM asset inventory process and this has been assessed by external auditors as part of iso27001 and SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance

Control Group	CID	Consensus Assessment Questions	IBM Response
Datacenter Security *Policy*	DCS-06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	See DCS-02.1
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role.
Datacenter Security *Secure Area Authorization*	DCS-07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	This is performed during the ordering process.
Datacenter Security *Unauthorized Persons Entry*	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	IBM Data center Physical security is controlled at many levels such as perimeter and building entrances, the physical security is not limited to, professional security staff, 24/7 video surveillance, security check point. Physical access points to the data halls all are recorded and monitored by onsite security, only authorized staff have the ability to access the data halls and they must authenticate a minimum of 2 times. Physical Security is reviewed by periodic internal audits as well as by third party audits such as FedRAMP, PCI, SOC, ISO27001 https://www.ibm.com/cloud-computing/bluemix/compliance
Datacenter Security *User Access*	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	
Encryption & Key Management *Entitlement*	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	IBM Cloud platform has defined a Key Management process to support encryption of data at rest and in transit for all IBM Cloud platform components. Customers may use their own customer managed keys for their applications deployed on IBM Cloud Foundry Runtimes using the UI as outlined here: https://developer.ibm.com/bluemix/2014/09/28/ssl-certificates-bluemixcustom-domains/ or using an API outlined here: http://bluemixapi-docs.stage1.mybluemix.net/swagger/?api=api-server - /default For IBM Cloud Container Service, all cluster configuration data is TLS encrypted in transit. For every cluster a default domain will be created and TLS key/cert is configured for ingress. Refer to ingress documentation for several different options including ability to use custom domain and the associated TLS configuration: https://console.bluemix.net/docs//containers/cs_apps.html#cs_apps_public_ingress
Encryption & Key Management *Key Generation*	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	All keys to manage the platform are managed by the IBM Cloud platform team and are recycled on a regular basis. Customers may use their own customer managed keys for their applications/containers deployed in IBM Cloud Foundry Runtimes and IBM Cloud Container Service. IBM Container Service provides and manages unique TLS certificates for default domains assigned for each cluster. Unique keys are issued to each dedicated tenant for VPN access.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	Customers may provide their own customer managed keys for their applications deployed on IBM Cloud platform which stores these securely for the customer. See these links for IBM Cloud platform Cloud Foundry runtimes and IBM Cloud Container Service respectively https://www.ibm.com/blogs/bluemix/2014/09/ssl-certificates-bluemix-custom-domains https://console.bluemix.net/docs//containers/cs_apps.html#cs_apps_public_ingress

Control Group	CID	Consensus Assessment Questions	IBM Response
	EKM-02.3	Do you maintain key management procedures?	IBM Cloud platform has Key Management policies which cover key lifecycle, key access and key strength. Access to keys are governed using the IBM Cloud platform access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. NIST recommendations for key strength and algorithms are followed. These policies have been audited by external auditors as part of iso27001 and SOC2 compliance certifications.
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	IBM Cloud platform has Key Management policies which cover key lifecycle. Access to keys are governed using an access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. For keys related to platform, only members of the key management team can generate, recycle or revoke keys and all actions are logged and sent to QRadar SIEM. Key management policies have been audited by external auditors as part of iso27001 and SOC2 compliance certifications.
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	The IBM Cloud platform uses an internal framework to create and manage keys and certificates. NIST recommendations for key strength and algorithms are followed. These policies have been audited by external auditors as part of iso27001 and SOC2 compliance certifications.
Encryption & Key Management *Encryption*	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	IBM Cloud platform Customer's are responsible for the encryption of their data at rest but IBM Cloud Data services provides a number of options to encrypt that data. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/data/ Disk Partitions where customer data resides are encrypted using LUKS.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	All IBM Cloud platform data is encrypted in transit. Data in transit encryption uses TLS from internet to the reverse proxy at edge of IBM Cloud platform network which terminates TLS. IPSEC based encryption is provided within the IBM Cloud platform network for all data in transit from the reverse proxy to IBM Cloud platform components. IBM Cloud platform customers must ensure their containers and applications are TLS enabled and can provide their own Certificates to manage that TLS termination. See EKM02.2 for details. Customers have different options on how they connect to their IBM Cloud platform dedicated instance, e.g. over public network or over a dedicated VPN with unique keys from their enterprise. This can apply to both end users of their applications and developers pushing new apps to IBM Cloud platform.
	EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	IBM Cloud platform Customer's are responsible for the encryption of their data at rest and may encrypt it before uploading to IBM Cloud Data storage. Customers may use their own customer managed keys for their applications deployed on IBM.

Control Group	CID	Consensus Assessment Questions	IBM Response
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	IBM Cloud platform has Key Management policies which cover key lifecycle, key access and key strength. Access to keys are governed using the IBM Cloud platform access governance tool that requires approval by user's manager and access owner, periodic revalidation for continued business need, and revocation on employee termination. NIST recommendations for key strength, and algorithm are followed.
Encryption & Key Management *Storage and Access*	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	All encryption algorithms in use are open/validated formats and are follow NIST.SP.800-57pt1 standards. Ciphers and protocols are reviewed on at least an annual basis and updated accordingly. A minimum of TLS 1.1. is mandated across IBM Cloud platform
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	IBM Cloud Foundry manages all keys for the platform in a proprietary store that meets NIST standards. Access is only available to members of the Key Management team with membership of that team being governed by IBM Cloud platform User Access governance. IBM Container Service manages all keys for the control plane in KeyProtect. Customers may use their own customer managed keys for their applications deployed on IBM Cloud Foundry runtimes and these are stored in a one-way process in a virtual key store which is not accessible by operations staff. For IBM Cloud Container service, the keys are stored as a kubernetes secret. Customers can use the Cloud Certificate Manager to store and manage their certs and these can be deployed as kubernetes secrets to the Container service Customers may encrypt their own data prior to storing in IBM Cloud Data storage and are responsible for storage of those encryption keys.
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	
Governance and Risk Management *Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	IBM Cloud platform maintains system baselines for all critical components and this had been verified by an independent auditor as part of ISO 27001 certification. IBM Cloud platform Customer applications are deployed in standard cloud foundry containers in hardened VM images.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Agents are deployed at OS level in all IBM Cloud platform machines and these check compliance with a set of security standards on a daily basis. Those security standards follow the IBM Cloud platform security policies and checklists which in turn align with iso27001 standards.

Control Group	CID	Consensus Assessment Questions	IBM Response
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	IBM Cloud platform applications are deployed in standardized cloud foundry containers. IBM Cloud Container service applications are deployed in standardized docker containers. Customers can use the IBM Cloud Container Registry to manage and deploy their own Docker images: https://console.bluemix.net/docs/services/Registry/index.html#index
Governance and Risk Management *Risk Assessments*	GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	Security logs are created for all critical operations in the IBM Cloud platform e.g. authentication, privileged operations, key management. These are available on request to all IBM Cloud platform dedicated and private customers for their dedicated environment. SOC2 and iso27001 reports are available on request and demonstrate the use of security controls in IBM Cloud platform. https://console.bluemix.net/docs/security/compliance.html#compliance Customers can use the IBM Cloud Log Analysis service to monitor their applications and containers deployed on IBM Cloud platform: https://console.bluemix.net/catalog/services/log-analysis
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	IBM Secure Engineering standard requires that threat modelling be carried out on at least an annual basis and part of that methodology is risk assessment. See https://www.ibm.com/security/secure-engineering/ IBM Cloud platform is iso27001 certified by external auditors. This certification has different control points which focus on risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html#compliance
Governance and Risk Management *Management Oversight*	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	IBM Security standards require managers to own the security and risks for their services and IBM Cloud platform is027001 certification the controls and processes in place to manage that. IBM Cloud platform managers must appoint a security focal to manage security and compliance for their component or service. IBM Secure Engineering standard requires all employees to take security education on an annual basis.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	IBM Cloud platform is iso27001 certified by external auditors with that certification being available to customers. Iso27001 is focused on security management processes and how IBM Cloud platform security processes map to iso27001 controls. https://console.bluemix.net/docs/security/compliance.html#compliance More detailed information on IBM Security processes can be made available to customers under NDA.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	IBM ISMP is reviewed on an annual basis.
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	IBM Cloud platform is iso27001 certified by external auditors with that certification being available to customers. As part of Iso27001 certification, controls and policies for service providers are reviewed. https://console.bluemix.net/docs/security/compliance.html#compliance
Governance and Risk Management *Policy*	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	IBM information security and privacy policies align with industry standards. Agreements are in place to verify and monitor supplier compliance with industry standards.. IBM Cloud platform is iso27001 certified by external auditors with that certification being available to customers. As part of Iso27001 certification, controls and policies for engaging with service providers are reviewed. https://console.bluemix.net/docs/security/compliance.html#compliance
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	

Control Group	CID	Consensus Assessment Questions	IBM Response
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards, certifications and/or regulations you comply with?	
Governance and Risk Management *Policy Enforcement*	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes, this is established by IBM Corporate HR policies, standards, training, and processes.
	GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes, this is established by IBM Corporate HR policies, standards, training, and processes.
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Regular risk assessments are conducted according to NIST800-53 standards. Policies, procedures and standards are subject to revision as a result of the holistic risk assessment as well as the risk assessments required as a part of the secure engineering process.
Governance and Risk Management *Policy Reviews*	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Tenants are notified of any change to their environment including those resulting from modified security policies. All deployments are controlled via IBM Cloud platform Change Management Policy and IBM Cloud platform/private customers are approvers for any changes that happen outside agreed maintenance windows.
	GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Security policies are reviewed at least annually. The privacy policy is updated and reviewed by the IBM Corporate Privacy Office.
Governance and Risk Management *Assessments*	GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Regular risk assessments are conducted according to NIST800-53 standards. These include likelihood and impact for all identified risks using qualitative and quantitative methods.
	GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Regular risk assessments are conducted according to NIST800-53 standards. This includes the independent consideration of all risk categories.
Governance and Risk Management *Program*	GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	IBM Secure Engineering standard mandates the use of threat modelling for all deployments which includes a risk assessment phase. https://www.ibm.com/security/secure-engineering/ IBM Cloud platform is iso27001 certified by external auditors. This certification is available to customers and has different control points which focus on quality assurance and risk assessment methodology. https://console.bluemix.net/docs/security/compliance.html#compliance
	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	
Human Resources *Asset Returns*	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	IBM Cloud platform has a security incident response plan which aligns with IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected security incident involving any IBM Cloud platform or Customer system or data. That scope covers any incidents related to privacy. Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/

Control Group	CID	Consensus Assessment Questions	IBM Response
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	IBM privacy policy is aligned with industry and country requirements and is continuously monitored for updates Refer to https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy
Human Resources *Background Screening*	HRS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	IBM Corporate HR policies dictate that all employment candidates are subject to background verification. IBM Cloud platform does not use contractors or other third parties to access client environments.
Human Resources *Employment Agreements*	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for IBM Cloud platform team members based on their role. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	IBM employees must acknowledge completion of training and this acknowledgment is documented and stored.
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	All employees of IBM sign NDA or confidentiality agreements regarding corporate and client information.
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Timely completion of the training program is a prerequisite to gaining access to customer data.
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Refer to https://www.ibm.com/security/secure-engineering/
Human Resources *Employment Termination*	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	IBM Corporate HR policies provide a baseline of standards for changes in, and termination of employment. The IBM Cloud platform access control tool queries the IBM Corporate system to detect any employee terminations on a daily basis.
	HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	IBM Corporate HR policies provide a baseline of standards for Access to IBM Cloud platform is managed vis IBM Cloud platform User Access Management tool which ensures role based access to any IBM Cloud platform system. Approval is required from both the employee manager and the system access owner and the process includes approval/continued business need and validation/revocation on employee termination.
Human Resources *Portable / Mobile Devices*	HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	IBM I.T. Security standards mandate that mobile devices are not permitted access to the customer environment. Privileged laptops are required for access to customer environments and owners of those laptops are required to install and maintain full disk encryption and other increased security controls.
Human Resources *Nondisclosure Agreements*	HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	All IBM Cloud platform policies and procedures are reviewed on at least an annual basis.
Human Resources *Roles / Responsibilities*	HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	All roles and responsibilities relating to information security and environment operations are documented for dedicated environments.
Human Resources *Acceptable Use*	HRS-08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	Refer to IBM Privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy

Control Group	CID	Consensus Assessment Questions	IBM Response
	HRS-08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	Refer to IBM Privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy
	HRS-08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	Customers can inform IBM to avoid further contact beyond fulfilling the customer request. Refer to the IBM privacy site. https://www.ibm.com/cloud-computing/bluemix/security-privacy#privacy
Human Resources *Training / Awareness*	HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/
	HRS-09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources *User Responsibility*	HRS-10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	IBM Secure Engineering standard mandates security education for all team members on an annual basis and that security education involves a formal registration that education is complete. In addition, IBM employees regularly receive notifications on the importance of cybersecurity, asset registration and asset security via email, online resources and other. Privileged laptops are required for access to customer environments or where the user is a privileges user for a particular regulatory requirement. Owners of those laptops are required to install and maintain full disk encryption and other increased security controls to satisfy regulatory standards.
	HRS-10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS-10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources *Workspace*	HRS-11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	Tenant and service level conflicts of interest are resolved via operational and management planning.
	HRS-11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. SOC2 compliance demonstrates the controls IBM Cloud platform has in place to safeguard against the unauthorized access or alteration of data stored in IBM Cloud platform. Security logs for all critical operations in the IBM Cloud platform are logged to the IBM QRadar SIEM. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to IBM Cloud platform QRadar. IBM personnel managing IBM Cloud platform QRadar are distinct from those having privileged access to IBM Cloud platform and this is enforced using IBM Cloud platform access governance tool.
	HRS-11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	IBM Cloud platform deploys standard hardened VM images to deploy new images. Access to VM image repositories is managed via an IBM Cloud platform User Access Management tool. Approval is required from both the employee manager and the system access owner and includes approval/continued business need and validation/revocation on employee termination. All changes must be approved by IBM Cloud platform Change Management process before being pushed to production. All changes and privileged actions to VM images are logged and sent to IBM QRadar SIEM.

Control Group	CID	Consensus Assessment Questions	IBM Response
Identity & Access Management *Audit Tools Access*	IAM-01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	All privileged users request operating system level, network device and IBM Cloud platform level access via an IBM Cloud platform User Access Management tool. Approval is required from both the employee manager and the system access owner. This provides the user with role based access to the requested system. Password policy per IBM IT standards are enforced for such accounts. IBM Cloud platform has daily reconciliation processes which verify that all privileged users are still valid in the IBM Employee directory. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
	IAM-01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
Identity & Access Management *User Access Policy*	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Privileged accesses to IBM Cloud platform is revoked on employee termination. There is a periodic revalidation for business need and reconciliation against target systems, and password policy per IBM IT standards are enforced for such accounts.
	IAM-02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	This process is tested through our external audits, and is tested repeatedly throughout the year.
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Dedicated secure networks are used for administration of IBM Cloud platform systems and these networks are segregated from the public networks through which customer user traffic flows.
Identity & Access Management *Policies and Procedures*	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	See IAM-01.1
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	See IAM-01.1
Identity & Access Management *Segregation of Duties*	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	IBM Cloud platform change management procedure defines clear lines between the groups that develop code and those that are permitted to deploy it after proper approvals. Access governance provides role based access to IBM Cloud platform production and the approval process requires a valid business.
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Access to source code repositories is managed via an IBM Cloud platform User Access Management tool. Approval is required from both the employee manager and the system access owner and includes approval/continued business need and validation/revocation on employee termination. All changes must be approved by IBM Cloud platform Change Management process before being pushed to production.
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Application developers are authenticated to IBM Cloud platform using IBM WebID or via SAML federation to a client provided identity provider or a client provided LDAP in the case of Dedicated and private IBM Cloud platform. OAuth based Cloud Foundry mechanisms to ensure each application developer only has access to the applications and service instances that they created.
	IAM-07.1	Do you provide multi-failure disaster recovery capability?	IBM Cloud platform provides a number of options to allow customers to deploy applications and containers for high availability including high availability zones within

Control Group	CID	Consensus Assessment Questions	IBM Response
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	a region and high availability across regions. https://www.ibm.com/developerworks/cloud/library/cl-multi-region-bluemix-apps-with-cloudant-and-dyn-trs/index.html https://www.ibm.com/developerworks/cloud/library/cl-high-availability-and-disaster-recovery-in-bluemix-trs/index.html https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations
	IAM-07.3	Do you have more than one provider for each service you depend on?	
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provided a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08.1	Do you document how you grant and approve access to tenant data?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. IBM Cloud platform has been audited by external auditors as part of SOC2 compliance and this includes controls IBM Cloud platform has in place to safeguard against the unauthorized access or alteration of data stored in IBM Cloud platform. https://console.bluemix.net/docs/security/compliance.html#compliance
	IAM-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	
Identity & Access Management *User Access Authorization*	IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	IBM Cloud platform privileged users request operating system level, network device and IBM Cloud platform level access via an IBM Cloud platform User Access Management tool. This access is used to deploy and manage new IBM Cloud platform environments and organizations and manage new IBM Container Service control plane environments Customers can appoint their own administrators to manage their IBM Cloud platform organizations, spaces and user roles as described in IBM Cloud platform documentation. https://console.bluemix.net/docs/admin/orgs_spaces.html For IBM Cloud Container Service, customers can appoint their own administrators to manage their clusters and cluster access management is described in documentation: https://console.bluemix.net/docs/containers/cs_cluster.html#cs_cluster_user

Control Group	CID	Consensus Assessment Questions	IBM Response
	IAM-09.2	Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	IBM Cloud platform privileged users request operating system level, network device and IBM Cloud platform level access via an IBM Cloud platform User Access Management tool. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM. These, and other controls evaluated as part of SOC2 certification, are designed to prevent unauthorized access to IBM Cloud platform data by IBM employees or other. Customers can appoint their own administrators to manage their IBM Cloud platform organizations, spaces and user roles as described in IBM Cloud platform documentation. https://console.bluemix.net/docs/admin/orgs_spaces.html For IBM Cloud Container Service, customers can appoint their own administrators to manage their clusters and cluster access management is described in documentation: https://console.bluemix.net/docs/containers/cs_cluster.html#cs_cluster_user
Identity & Access Management *User Access Reviews*	IAM-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Privileged accesses to IBM Cloud platform has a periodic revalidation for business need and reconciliation against target systems and access is revoked on employee termination. The process is tested by external auditors as part of SOC2 controls. https://console.bluemix.net/docs/security/compliance.html#compliance
	IAM-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Inappropriate entitlements trigger a security defect in the IBM Cloud platform ticketing system and that tracks the actions taken on user ids and their entitlements.
	IAM-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Where there is suspected inappropriate access to a customer system or customer data, IBM Cloud platform notifies the IBM Cybersecurity Incident Response Team (CSIRT) and the CSIRT process includes analysis, forensics and root cause analysis for the security incident IBM legal are involved and the customer is kept informed at all stages. The IBM Cloud platform status page https://developer.ibm.com/bluemix/support/#status is used for all client notifications including "general" security related notifications. Security notifications point to IBM security bulletins published per the IBM Product Security Incident Response Team (PSIRT) (https://www.ibm.com/security/secure-engineering/process.html) process.

Control Group	CID	Consensus Assessment Questions	IBM Response
Identity & Access Management *User Access Revocation*	IAM-11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Privileged accesses to IBM Cloud platform has a periodic revalidation for business need and reconciliation against target systems and access is revoked on employee termination. The process is tested by external auditors as part of SOC2 controls. https://console.bluemix.net/docs/security/compliance.html#compliance
	IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	
Identity & Access Management *User ID Credentials*	IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	]IBMid is the IBM Identity Service, a cloud-based identity access and management solution that provides identity and single sign-on services for IBM Cloud and IBM applications IBM Cloud platform supports authentication to IBM Cloud platform for application developers via SAML federation to a client provided identity provider or a client provided LDAP or SAML identity provider in the case of Dedicated and private IBM Cloud platform. IBM Cloud platform SSO services allows developers to provide SSO for their users to IBM Cloud platform applications and services. Refer to the SSO section in 'Securing Workloads in IBM Cloud' white paper https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/applications/#sso
	IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	IBM Cloud platform (Public) supports delegation authentication to a number of social identity sources Refer to the SSO section in 'Securing Workloads in IBM Cloud' white paper https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/applications/#sso
	IAM-12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	IBM Cloud platform supports authentication to IBM Cloud platform for application developers via SAML federation to a client provided identity provider or a client provided LDAP or SAML identity provider in the case of Dedicated and private IBM Cloud platform.
	IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	This can be enforced for IBM Cloud platform Dedicated tenants at tenant requests.
	IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Role based identity management can be provided via SAML federation to a client provided identity provider IBM Cloud platform provides role based access to organizations, spaces and applications which is enforced using Oauth. Organization administrators for a customer can configure which roles and access different people within their organisation(s) have. https://console.bluemix.net/docs/iam/iamusermanage.html#iamusermanage
	IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	IBM Cloud platform supports authentication to IBM Cloud platform for application developers via SAML federation to a client provided identity provider. That identity provider may support any type of authentication including multi-factor.
	IAM-12.7	Do you allow tenants to use third-party identity assurance services?	IBM Cloud platform supports authentication to IBM Cloud platform for application developers via SAML federation to a client provided identity provider which can provide third-party identity assurance services.
	IAM-12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	IBM Id supports strong password policy enforcement including minimum password length, password history and password lockout. IBM Cloud platform Customers can enforce any password policy they choose by using saml federation.
	IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	IBM Cloud platform Customers can enforce any password policy they choose by using saml federation.
	IAM-12.10	Do you support the ability to force password changes upon first logon?	IBM Cloud platform Customers can enforce any password policy they choose by using saml federation.

Control Group	CID	Consensus Assessment Questions	IBM Response
	IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	IBM Id supports password reset and unlocking accounts. https://www.ibm.com/ibmid/password1.html?
Identity & Access Management *Utility Programs Access*	IAM-13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	IBM Cloud infrastructure and IBM Cloud platform restrict access to administrative tools and utilities via an IBM Cloud platform User Access Management tool and access is based on least privilege and best practices. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM.
	IAM-13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	Access to Virtual Infrastructure is restricted to only personnel who require access and all access is logged. Monitoring and controls have been reviewed by independent auditors as part of SOC2 audits. https://console.bluemix.net/docs/security/compliance.html#compliance
	IAM-13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	All IBM Cloud platform systems are security hardened which includes File Integrity Monitoring in Cloud Foundry to detect changes on critical files. For the Container Service, If you have a standard cluster, you can use Kubernetes daemon sets for everything that you want to run on every worker node including File Integrity Monitoring. Dedicated IBM Cloud platform with direct internet facing endpoints includes IPS which examines incoming traffic and detects known malware signatures. Those signatures are updated automatically from the IPS vendor. All logs are delivered to IBM QRadar SIEM and rules are enabled for intrusion detection and generation of security alerts.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Security logs for all critical operations in the IBM Cloud platform are logged to the IBM QRadar SIEM. Tampering of logging configuration and security logs are logged themselves and such logs are delivered to IBM Cloud platform QRadar. IBM personnel managing IBM Cloud platform QRadar are distinct from those having privileged access to IBM Cloud platform and this is enforced using IBM Cloud platform access governance tool.
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	External auditors have affirmed that IBM Cloud platform controls are operating effectively against a number of standards including ISO27001/2, SSAE16 SOC2 and others. https://console.bluemix.net/docs/security/compliance.html#compliance
	IVS-01.4	Are audit logs centrally stored and retained?	Security logs for all critical operations in the IBM Cloud platform are logged to the IBM QRadar SIEM. Security logs are retained for one year.
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	BM QRadar SIEM is configured with a set of rules which trigger offences based on incoming log events. Those offences trigger pager duty alerts to the IBM Cloud platform SOC team on a 24x7 basis. Refer to the IBM QRadar documentation for more details. https://www.ibm.com/security/security-intelligence/QRadar/
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	IBM Cloud platform deploys standard hardened VM images to deploy new images. All changes and privileged actions to VM images are logged and sent to IBM QRadar SIEM.
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	IBM Cloud infrastructure provides a NTP service which IBM Cloud platform uses. It uses dedicated radio receivers to pick up signal directly from a stratum 0 source. In turn, that means these servers feed off a stratum 1 source (our internal servers).

Control Group	CID	Consensus Assessment Questions	IBM Response
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	System capacity requirements for Dedicated customers are negotiated contractually.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	IBM Cloud infrastructure maintains capacity and resource planning in alignment with ISO27001 and these efforts are validated by external auditors. IBM Cloud platform deploys applications in cloud foundry containers which are limited in terms of CPU, memory and other resource usage. The number of containers per host machine is limited.
	IVS-04.3	Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	IBM Cloud platform projects the anticipated capacity for the platform and ensures there is enough hardware, memory and other resources to meet that anticipated capacity. Based on the current and anticipated capacity, warning limits are in place which trigger alerts to operations when breached. That triggers another cycle of capacity planning and new warning limits. For IBM Cloud platform Dedicated and private, details of the current capacity usage are made available to the customer via the IBM Cloud platform Operations console.
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	The IBM Secure Engineering standard dictates multiple scanning techniques be used against production systems. These include automated dynamic scans, manual penetration tests and threat modelling. These activities both the virtualization technologies and all Virtual machines and containers deployed on those virtualization technologies. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	IBM Cloud platform does not offer IaaS. However, IBM Cloud does provide guidance on how to create a layered security architecture equivalence using your virtualized solution. Refer to this white paper on securing workloads in IBM Cloud. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Network architectures are regularly reviewed and updates are made after any significant change.
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	IBM Cloud platform conducts reviews on all firewalls on a quarterly basis. These reviews check for appropriateness of access and any unauthorized changes made outside of the IBM Cloud platform change control process. These firewall reviews have been assessed by external auditors as part of SOC2 compliance. https://console.bluemix.net/docs/security/compliance.html#compliance IBM Cloud Containers service may use firewalls or calico policies to provide layer 3 manage interface access. Changes to these policies are tracked and deployed using github and require 2 levels of approvals prior to deployment and ensures the policy rules are always in syn with approved changes. IBM I.T. standard mandates an annual review of IBM Cloud platform network architecture. This is performed by an independent team from IBM CISO office and includes checks for appropriateness of access.
	IVS-06.4	Are all firewall access control lists documented with business justification?	All changes to IBM Cloud platform firewalls must follow the IBM Cloud platform change controls process which requires business justification and multiple levels of review and approval before deployment. IBM Cloud platform conducts reviews on all firewalls on a quarterly basis which check for any unauthorized changes made outside of the IBM Cloud platform change control process. Changes to calico policies are tracked in github along with business justification and approvals

Control Group	CID	Consensus Assessment Questions	IBM Response
Infrastructure & Virtualization Security *OS Hardening and Base Conrols*	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	All host machines in IBM Cloud platform are deployed as standard builds which remove unnecessary ports, protocols, and services. Agents deployed to all machines hosting customer traffic check for compliance with a set of hardening rules on a daily basis.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Dedicated IBM Cloud platform tenants can provision production and non-production environments via requests, as limited by their contracts.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	IBM Cloud platform does not offer IaaS.
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	IBM Cloud platform has a non-production environment for both Public and Dedicated IBM Cloud platform used to perform any testing pre-deployment to production environment. The non-production environments are logically segregated from production environments All IBM Cloud platform dedicated environment are logically segregated and are deployed on dedicated hardware.
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	All systems and resources are protected by at least one firewall. IBM Cloud container service clusters may be protected by a firewall or calico policies which are a layer 3 managed interface.
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	All systems and resources in IBM Cloud Foundry and all control plane traffic in IBM Container Service are protected by at least one firewall. Firewall configurations and firewall reviews are assessed by external auditors as part of the applicable compliance standard. https://console.bluemix.net/docs/security/compliance.html#compliance For IBM Cloud Containers clusters, customers are responsible for their firewall policies and may use vyatta or other firewall or calico policies to provide layer 3 manage interface access.
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	In a dedicated environment, the customer has the option to create separate production and non production environments and would have the responsibility to manage the firewall between them.
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	All systems and resources are protected by at least one firewall or managed interface
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	All IBM Cloud platform data is encrypted in transit. IBM Cloud platform does not manage any physical servers. IBM Cloud platform customers are responsible for any transfer of their data and ensuring it is encrypted.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	IBM Cloud platform privileged users request access to IBM Cloud platform environments, including administrative tools, hypervisors and virtual machines, via an IBM Cloud platform User Access Management tool. Approval is required from both the employee manager and the system access owner. All successful and failed logins and all privileged actions are logged and sent in near real-time to IBM QRadar SIEM. These, and other controls evaluated as part of SOC2 certification, are designed to prevent unauthorized access to IBM Cloud platform data by IBM employees or other. All systems and resources are protected and isolated by at least one firewall. All access to administrative consoles, hypervisors and Virtual Machines is over TLS and all IBM Cloud platform data is encrypted in transit.

Control Group	CID	Consensus Assessment Questions	IBM Response
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	IBM Cloud platform does not have access to physical Ethernet ports, and does not have the ability to implement wireless in the environment. IBM Cloud infrastructure does not permit the use of wireless networks and scans for and rogue devices are conducted routinely. These controls have been accessed by and independent auditor as part of PCI DSS AoC and can be made available to customers upon request.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	IBM Cloud platform network diagrams clearly document the boundaries of different environments and systems including the IBM Cloud platform data flows across boundaries. IBM Cloud platform customers are responsible for their own data including any compliance with any legal standards for that data. The IBM CISO office conduct an annual review of the IBM Cloud platform network architecture which includes checks on classification of IBM Cloud platform data, network zones and protections between zones.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Firewalls, or optionally calico policies for Container service, restrict traffic from the internet to ports 80 and 443. IBM Cloud platform dedicated customers are responsible for specifying firewall rules in their environment and may request changes to lock down that outbound access either to the internet or via a VPN to their enterprise network. IBM Cloud platform intrusion detection is provided by a combination of IBM Cloud infrastructure provided capabilities (for Public and Dedicated IBM Cloud platform environments that run on IBM Cloud infrastructure), capabilities at the perimeter level within firewall/DataPower and by monitoring of security logs that are consolidated within the IBM QRadar SIEM tool. Periodic scanning to detect OWASP issues are done for the IBM Cloud platform endpoints.
Interoperability & Portability *APIs*	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	A list of APIs for IBM Cloud Foundry runtimes is available at: https://www.ibm.com/cloud/cloud-foundry/resources A list of APIs available for IBM Cloud Container service at: https://containers.bluemix.net/swagger-api/#/
Interoperability & Portability *Data Request*	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	IBM Cloud platform customers are responsible for the data including the format of that data and how and when it is accessed.
Interoperability & Portability *Policy & Legal*	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Policies and procedures are in place governing the use of APIs between IBM Cloud platform and third party applications.
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	IBM Cloud platform customers are responsible for the data including how and when that data is migrated. Refer to the IBM Cloud platform Data Services documents to understand how these can assist with data migration https://console.bluemix.net/docs/

Control Group	CID	Consensus Assessment Questions	IBM Response
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	All IBM Cloud platform data is encrypted in transit. See AIS04.1
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	IBM Cloud uses portable standards and details are provided in online documentation. https://www.ibm.com/developerworks/cloud/library/cl-tools-to-ensure-cloud-application-interoperability/index.html https://console.bluemix.net/docs/containers/container_index.html#container_index
Interoperability & Portability *Virtualization*	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	IBM Cloud platform uses industry standard virtualization formats to help ensure interoperability, such as Docker Containers, Cloud Foundry and VMWare.
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	IBM Cloud infrastructure do not have solution specific virtualization hooks.
Mobile Security *Anti-Malware*	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	IBM Secure Engineering standard mandates security education for all team members on an annual basis. Additional security education is required on a periodic basis for team members based on their role. Anti-malware awareness training, specific to mobile devices, is included in that training.
Mobile Security *Application Stores*	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	A list of approved application stores is available and has been communicated to users.
Mobile Security *Approved Applications*	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	IBM Corporate Security mandates the installation of a Mobile Device Management client on all BYODs used for IBM business. That client ensures compliance with IBM Corporate security standards including ensuring that only approved application stores can be used.
Mobile Security *Approved Software for BYOD*	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	The IBM Corporate security policy clearly states which applications and application stores are approved. Mobile Device Management is in place to block risky extensions and plugins.
Mobile Security *Awareness and Training*	MOS-05	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Cloud Based Services*	MOS-06	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	IBM Corporate security policy defines the pre-approved vendor(s) for cloud storage on mobile devices with regards to company business data.
Mobile Security *Compatibility*	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	IBM Corporate security policies define these elements, which are enforced by a required mobile device management tool.
Mobile Security *Device Eligibility*	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	IBM Corporate security policies define the eligibility requirements to allow for BYOD usage. BYOD is not permitted to connect to customer environments or to store customer data.
Mobile Security *Device Inventory*	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	Mobile devices are not permitted to connect to customer environments or to store customer data. IBM Corporate retains control of inventories, forced patching, etc., of mobile devices.
Mobile Security *Device Management*	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	Mobile devices are required to install a mobile device management tool. No mobile devices are permitted to store, transmit or process customer data.
Mobile Security *Encryption*	MOS-11	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	IBM Corporate security policies require full device encryption on mobile devices as well as BYOD. Sensitive data is not permitted on mobile devices or on BYOD.

Control Group	CID	Consensus Assessment Questions	IBM Response
Mobile Security *Jailbreaking and Rooting*	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	Mobile devices are required to install a mobile device management tool. Jailbreaking or rooting is prevented and reported on.
	MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	Mobile devices are required to install a mobile device management tool. Jailbreaking ,rooting, or circumventing required controls is prevented and reported on.
Mobile Security *Legal*	MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	IBM Corporate Security Policies define these elements for BYOD.
	MOS-13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	BYOD are required to install a mobile device management tool. Jailbreaking ,rooting, or circumventing required controls is prevented and reported on.
Mobile Security *Lockout Screen*	MOS-14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	Automatic lockouts are configured for BYOD and mobile devices.
Mobile Security *Operating Systems*	MOS-15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	IBM Cloud platform does not develop, approve or deploy mobile device operating systems or applications. IBM Corporate manages these items through change management processes and enforces them through a mobile device management tool.
Mobile Security *Passwords*	MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	All mobile devices and BYOD have required passwords.
	MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?	Passwords are enforced through a mobile device management tool.
	MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	Authentication requirements for passwords residing on the device, e.g. screen pin, can't be changed and this is enforced by a mobile device management tool.
Mobile Security *Policy*	MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	Data is stored on the cloud thus the corporate data is backed up. There is no device resident data except for authentication keys.
	MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	BYOD mobile devices are not permitted to use unapproved application stores.
	MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	Anti-malware is required on BYOD and enforced via management tools.
Mobile Security *Remote Wipe*	MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	All mobile devices have remote wipe configured through the required mobile device management tools.
	MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	All mobile devices have remote wipe configured through the required mobile device management tools.
Mobile Security *Security Patches*	MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	All mobile devices are configured to force installation of security patches deemed critical by the IBM Office of the CIO.
	MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	All mobile devices are configured to force installation of security patches deemed critical by the IBM Office of the CIO, through the Mobile Device Management Tool.
Mobile Security *Users*	MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	The policy clearly states mobile devices and BYOD systems are not permitted to access customer environments.
	MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	The policy clearly states mobile devices and BYOD systems are not permitted to access customer environments. Users whose primary role is accessing or maintaining customer devices must use a company provided privileged workstation.

Control Group	CID	Consensus Assessment Questions	IBM Response
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	IBM Cybersecurity and IBM Legal maintain relationships with the proper local authorities.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	IBM Cloud platform has a security incident response plan which aligns with IBM Cybersecurity Incident response process and the IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected security incident involving any IBM Cloud platform or Customer system or data. Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	The IBM Cybersecurity Incident Response team (CSIRT) are engaged wherever there is a suspected a suspected security incident involving any IBM Cloud platform or Customer system or data. One of their responsibilities is to engage with the customer and keep them informed on the investigation, findings and any root cause analysis actions.
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	Refer to Security Incident Response Management in the 'Securing Workloads in IBM Cloud' whitepaper. https://developer.ibm.com/cloudarchitecture/docs/security/securing-workloads-ibm-cloud/intelligence-monitoring/
	SEF-02.4	Have you tested your security incident response plans in the last year?	The Security incident response plan is reviewed and tested at least annually.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	Security logs for all successful and failed login attempts and all critical operations in the IBM Cloud platform, including network devices, host machines and IDS logs, are logged to IBM QRadar SIEM. IBM QRadar SIEM is configured with a set of rules which trigger offences based on incoming events across all log sources. Those offences trigger pager duty alerts to the IBM Cloud platform SOC team on a 24x7 basis. Refer to the IBM QRadar documentation for more details. https://www.ibm.com/security/security-intelligence/QRadar/
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	For IBM Cloud platform dedicated and private environments, the potential incident activities are always attributed to a specific environment belonging to a customer. For Public IBM Cloud platform, investigation of the incident may be required to determine which customer(s) was involved.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Specific details regarding chain of custody, forensics, and litigation holds are addressed by IBM Legal and the IBM Cybersecurity Incident Response Team (CSIRT).
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	

Control Group	CID	Consensus Assessment Questions	IBM Response
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Security logs for all successful and failed login attempts and all critical operations in the IBM Cloud platform, including network devices, host machines and IDS logs, are logged to IBM QRadar SIEM. IBM QRadar SIEM provides reports on the types and volumes of all security events and all offences triggered based on QRadar rules. All security incidents triggering the IBM Cloud platform Security incident response plan have a root cause analysis which record impact and trigger actions to mitigate in future.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	For IBM Cloud platform dedicated and private environments, details of those offences can be shared upon request via reports delivered to their IBM operations console. The IBM Cloud platform status page is used for all client notifications including "general" security related notifications: https://developer.ibm.com/bluemix/support/#status. Security notifications point to IBM security bulletins published per the IBM Product Security Incident Response Team (PSIRT) process. https://www.ibm.com/security/secure-engineering/process.html
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	IBM Cloud platform customers are ultimately responsible for the data integrity of their workload. IBM Cloud platform compliance certifications demonstrate the controls IBM Cloud platform has in place to provide a secure platform including controls related to supply chain. https://console.bluemix.net/docs/security/compliance.html#compliance
	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	Refer to IAM 10.3
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	IBM Cloud platform projects the anticipated capacity for the platform and ensures there is enough hardware, memory and other resources to meet that anticipated capacity. Based on the current and anticipated capacity, warning limits are in place which trigger alerts to operations when breached. That triggers another cycle of capacity planning and new warning limits.

Control Group	CID	Consensus Assessment Questions	IBM Response
	STA-03.2	Do you provide tenants with capacity planning and use reports?	For IBM Cloud platform Dedicated and private, details of the current capacity usage are made available to the customer via the IBM Cloud platform Operations console.
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Internal audits are conducted on at least an annual basis and check conformance and effectiveness of IBM Cloud platform policies, procedures, and supporting measures and metrics.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.3	Does legal counsel review all third-party agreements?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	IBM Legal and Procurement designate the requirements for the establishment and maintenance of supplier relationships.
	STA-05.5	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	IBM maintains all required sub-processing agreements and makes them available as required to clients upon request.
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06.1	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	IBM has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements. IBM supplier management processes are validated by external auditors as part of compliance with SOC and ISO27001.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	IBM maintains formal agreements with third party suppliers and those agreements are reviewed on an annual basis. Supplier relationships and processes are reviewed by an independent auditor as part of SOC2 compliance.
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	External audit assurance reports are reviewed for key suppliers on at least an annual basis.
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	External audit assurance reports are reviewed for key suppliers on at least an annual basis.

Control Group	CID	Consensus Assessment Questions	IBM Response
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Penetration testing is allowed by IBM Cloud platform on their own Dedicated and private environments with approval of IBM Cloud CISO.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Pen testing for Public and Dedicated IBM Cloud platform is performed on an annual basis using a 3rd party vendor. Penetration testing for Dedicated IBM Cloud platform will only be performed and scheduled with the approval of the customer and penetration test and vulnerability scan reports can be made available upon request for their own Dedicated IBM Cloud platform environments.
Threat and Vulnerbility Management *Antivirus / Malicious Software*	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Antivirus Antimalware protection is deployed on all Windows systems at the host level and reports back to a central console managing Antivirus Antimalware. Automated updates are in place for new malware or virus signatures. All Linux systems are deployed using a pre-hardened image that is patched to the latest operating system level patches using BigFix, and they are hardened per the operating system hardening specification. The IBM GSSD team guidelines are used to determine severity of operating systems patches so they can be applied in a timely manner per our patch management policy. The following secondary controls are in place to protect against malware 1. All systems are security hardened which includes File Integrity Monitoring in Cloud Foundry to detect changes on critical files. 2. Dedicated IBM Cloud platform with direct internet facing endpoints includes IPS which examines incoming traffic and detects known malware signatures. Those signatures are updated automatically from the IPS vendor. 3. All privileged access is approved by a user's manager and an access approver, is periodically revalidated, and is revoked on user transfer or employee termination. 4. Change Management: All changes to software on systems must be approved by a reviewer and a manager. 5. Patch management is fully automated using IBM BigFix. Container Service customers can set up secure Docker images in the IBM Cloud Container Registry. Vulnerability Advisor is a component of IBM Cloud Container Registry that scans for potential vulnerabilities, makes security recommendations, and provides instructions to resolve vulnerabilities 6. QRadar: rules on security logs from systems are enabled for malware detection and generation of security alerts. 7. PSIRT: processes enforced to update any systems or software with potential malware vulnerabilities. 8. NESSUS: vulnerability scans are run periodically against all public and private endpoints.
	TVM-01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	

Control Group	CID	Consensus Assessment Questions	IBM Response
Threat and Vulnerbility Management *Vulnerability / Patch Management*	TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Secure Engineering Standard ensure security as part of our SDLC. Those standards include processes for secure coding, vulnerability assessment, vulnerability scanning, penetration testing, education, processes for 3rd party code approval and threat modelling. The standards used are regularly evaluated and updated for inclusion or replacement. Refer to https://www.ibm.com/security/secure-engineering/ Network based vulnerability scans are run periodically using Nessus.
	TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Secure Engineering Standard mandates vulnerability assessment which requires automated code and application scanning in addition to manual testing. Dynamic and static code scanning is performed using IBM Appscan on a monthly basis or whenever there is a major change. Manual reviews are performed for security related code and reviews check against OWASP top ten vulnerabilities.
	TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	The IBM Product Security Incident Response Team (PSIRT) process is followed for security incident management (https://www.ibm.com/security/secure-engineering/process.html). The PSIRT team monitor and alert on any vulnerabilities discovered in any IBM system including at OS level and each IBM Cloud platform and Service has assigned PSIRT Responders to act on those vulnerabilities. SLAs are in place to ensure timely assessment on whether each component is vulnerable and subsequent patching, with the SLAs varying depending on the CVSS score. Nessus scans are run periodically and check for any OS level vulnerabilities detected from network scans.
	TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?	IBM Cloud platform dedicated and private customers can request details of Vulnerability scans for their dedicated environments. These are provided via the IBM operations console.
	TVM-02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	IBM Bigfix is used for managing and automating patching across IBM Cloud platform. This provides full visibility on what is patched in addition to providing the automation to push out the patches to all machines across all IBM Cloud platform environments. Refer to these public docs. https://www.ibm.com/marketplace/bigfix-patch-management
	TVM-02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	IBM Cloud platform dedicated and private customers can be provided with details of risk-based systems patching time frames upon request.

Control Group	CID	Consensus Assessment Questions	IBM Response
Threat and Vulnerbility Management *Mobile Code*	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	IBM Cloud platform has a Change Control process to manage and track changes to any portion of the system, regardless of its maturity level (Experimental, Beta or GA). The change control process requires multiple levels of review approval including component owners and management. For customer private clouds, the changes will only be made during an agreed change window or with the explicit approval of the customer and no changes are made without informing the customer in advance. For Cloud Foundry, File integrity monitoring runs on all VMs in customer environments and tracks any unauthorized changes to that VM such as identity management, networking, system management and OS configuration. For the Container Service, If you have a standard cluster, you can use Kubernetes daemon sets for everything that you want to run on every worker node including File Integrity Monitoring.
	TVM-03.2	Is all unauthorized mobile code prevented from executing?	

IBM Cloud services Response to the Cloud Security Alliance Cloud Control Matrix v3.0.14

http://www.ibm.com/trust

IBM Cloud Services Response to the Cloud Security Alliance Cloud Control Matrix

The Cloud Security Alliance (CSA) is a not-for-profit organization promoting the use of best practices for security assurance within cloud computing. The CSA published the Cloud Control Matrix to support customers in the evaluation of cloud providers and to identify questions prudent to have answered before moving to cloud services.

Learn more: https://cloudsecurityalliance.org/

Version 1, Published July 2018

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Contents

Introduction

IBM Cloud is the cloud for smarter business. A faster, more secure journey to cloud trusted by thousands of enterprises, across 20 industries. With IBM Cloud you have more ways to migrate, modernize and build innovative cloud apps today, and unlocking the value of all your data with analytics, machine learning, and AI.

IBM Cloud services is a portfolio of hundreds of services built on the IBM Cloud and designed to meet the needs of customers worldwide. All IBM Cloud services are managed with a common security framework and part of a centralized ISO/IEC 27001:2013 Certified Information Security Management System (ISMS) that provides an internationally recognized information security program and controls that are selected across industry best practices such as ISO /IEC 27002, 270017, 27018, NIST Special Publication 80-53r4. These responses to the Cloud Security Alliance Cloud Control Matrix address the security controls in place for the IBM Cloud services that are part of this centralized ISMS. Download the ISO certificate for a full list of the in-scope IBM Cloud services.

IBM has published additional documents, covering other IBM Cloud solutions, on the CSA Star website at https://cloudsecurityalliance.org/registry/ibm-cloud/

Learn more about IBM Cloud and IBM Cloud services at https://www.ibm.com/cloud/yourcloud/

Learn more about IBM's approach to trust and compliance at: http://www.ibm.com/trust

Audit Assurance & Compliance

Control ID in CCM	Control Description	IBM Cloud Services Response
AAC-01	*Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.*	IBM maintains a rigorous program of internal audits, quarterly KPI checking, and semi-annual external audits. The audit program is part of the executive management approval and review process. Offerings are certified annually to ISO 27001 or SAE SOC 2 or both, or as stated in the relevant Transaction Document. IBM provides certifications, attestations, audit reports, and other supporting materials to its clients, which verify and demonstrate IBM's adherence to its legal and contractual obligations.
AAC-02	*Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.*	Independent reviews and audits are conducted at least annually. Risk assessment and treatment plans are a key part of these reviews. The results are reviewed by executive management and action plans put in place, approved by management, implemented and tracked to completion. Non-conformities from previous cycles are checked in subsequent internal audits and corrective actions are reviewed during external (certification surveillance) audits.
AAC-03	*Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.*	The IBM Cloud services ISMS control framework captures the legal, regulatory and contractual obligations of the IBM Cloud services. The ISMS is reviewed and updated at least annually to maintain continuous improvement, and to ensure that any updates to IBM's adopted standards and legal obligations are properly addressed.

Application & Interface Security

Control ID in CCM	Control Description	IBM Cloud Services Response
AIS-01	*Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.*	IBM maintains policies and procedures to govern and verify that its Cloud Service applications and APIs are developed, deployed, tested, and maintained using industry and internal standards. IBM's secure engineering and privacy by design guidelines provide high standards for IBM's security and privacy practices, including architecture and code reviews; risk assessment and remediation; pre and post deployment security testing, including regular vulnerability scanning and penetration testing; security information and event logging and monitoring; automated security configuration verification and management; and identity and access management. In addition to ensuring a consistently high level of security for IBM Cloud Services, such reviews, monitoring, and testing, configuration and identify management, and internal and external audits, provide regular confirmation of IBM's adherence to its legal obligations and stated technical and organizational security and privacy measures.
AIS-02	*Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.*	Clients are responsible for determining whether a standard IBM Cloud Service is suitable for their use, and are required to review and agree with the terms of the relevant Cloud Service, including its stated security and privacy measures, prior to use. Security and privacy terms for IBM Cloud Services are provided in the base contractual agreement, including Data Security and Privacy Principles for IBM Cloud Services, the Data Processing Addendum for information subject to the EU General Data Protection Regulation (GDPR), and relevant Transaction Documents, such as the Service Description, order document, and associated attachments.

Application & Interface Security

Control ID in CCM	Control Description	IBM Cloud Services Response
AIS-03	*Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.*	IBM maintains standard procedures and implementation guidelines to verify the proper implementation of controls throughout its design, development, and operational lifecycles, including secure engineering and privacy by design guidelines, secure deployment checklists, and adherence to the IBM Secure Engineering Framework. The use of technical measures such as input sanitization, output validation, encryption in transit and at rest, checksums, hashes and other integrity checks, coupled with business continuity measures and extensive logging and monitoring, are designed, implemented, and maintained to protect against systemic processing errors, data loss or corruption, and misuse of information.
AIS-04	*Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.*	IBM maintains corporate policies and standards which support data and system security, privacy, confidentiality, integrity and availability, and apply to all IBM cloud services. Each IBM cloud service implements standard controls and processes in compliance with IBM's corporate policies, and is subject to accredited third-party validation against standards, such as ISO 27001, ISO 27017, ISO 27018, SSAE SOC 2, FedRAMP, HIPAA, and PCI-DSS, to the extent stated in the relevant service description. Compliance with legal, regulatory and contractual obligations is mandatory for all IBM cloud services and checks for updates to such obligations are performed regularly. Revisions to the associated policies, controls, and terms are incorporated as required and appropriate.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-01	*A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.* *Requirements for business continuity plans include the following:* *• Defined purpose and scope, aligned with relevant dependencies* *• Accessible to and understood by those who will use them* *• Owned by a named person(s) who is responsible for their review, update, and approval* *• Defined lines of communication, roles, and responsibilities* *• Detailed recovery procedures, manual work-around, and reference information* *• Method for plan invocation*	IBM maintains written corporate directives that establish a framework for business continuity standards, including roles and responsibilities for oversight of compliance with such standards. The framework includes guidelines for understanding the IBM organization, business continuity roles & responsibilities, actions to address business continuity risk, plan documentation, testing, and maintenance. Further, each business unit assigns an executive business continuity management sponsor who is responsible for providing corporate guidance to the business unit, and for overseeing the business unit's enactment of and compliance with IBM's directives, policies, and implementation guidelines. All of the requirements in this CSA-CCM control are addressed in IBM's corporate directives, standards, policies and implementing procedures. Complete plans, documents, checklists, and training are made available to the personnel who have responsibilities for business continuity efforts.
BCR-02	*Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.*	Business continuity plans define roles and responsibilities and detailed procedures for recovery per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed and tested at least annually, using testing exercises that follow industry standard practices, to assess their effectiveness in an adverse situation. Appropriate stakeholders are involved in testing. Plans are updated as appropriate in support of continuous improvement using test output, findings, and lessons learned. Test results are reviewed, and corrective actions are taken as appropriate, and plans and processes are updated according to lessons learned.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-03	*Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.*	IBM Cloud Service data centers have controls in place to protect against environmental threats such as excessive ambient temperature, fire, flood, and humidity. Further, controls are in place to mitigate the risk of utility failures, such as utility redundancy, backup power, 24x7x365 monitoring, and automatic fail-over switching. Implemented controls are tested regularly and audited in both IBM internal and external third-party audits.
BCR-04	*Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:* *• Configuring, installing, and operating the information system* *• Effectively using the system's security features*	Policies, procedures and other documentation needed to install, configure and operate the IBM Cloud service, including all security features (e.g. encryption, firewalls, identity and access management, intrusion detections and prevention, and monitoring), are disseminated to IBM personnel who have access to the offering information systems. All documents are located in the IBM Cloud service documentation repository and are only available to authorized personnel using role-based access. All policies, processes, and/or procedures are consistent with the requirements of applicable laws and regulations; corporate directives, policies, and adopted standards; and contractual agreements.
BCR-05	*Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.*	IBM data centers have physical protections in place to protect against threats of natural and man-made disasters and civil disturbances. Protective measures and controls are audited and certified at least annually for compliance with SSAE SOC 2 and ISO 27001, or as stated in the relevant transaction document.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-06	*To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.*	The IBM data center site selection process includes assessment of environmental threats, hazards, and opportunities for unauthorized access. Further, all IBM data center locations maintain measures to mitigate risks to the information processing systems from environmental conditions such as fire, flood, and storms, and from unauthorized access to secure areas. Redundant and disaster recovery sites are selected on a number of criteria including geographic location and proximity to other data center locations. Implemented measures are audited both internally and in external third-party audits for ISO 27001 and SSAE SOC 2 certification.
BCR-07	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.*	Equipment maintenance activities adhere to the supplier's recommendations and are performed by only authorized personnel. Comprehensive records are kept and change management procedures strictly followed. Policies are established to help maintain the continuity and availability of operations and support personnel, including redundant links, replication, and automatic failover, to ensure hardware maintenance activities are transparent to cloud service subscribers and end users.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-08	*Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.*	Physical and Environmental Protection controls are in place in all IBM data centers and are regularly audited in both internal and external third-party audits, such as ISO27001 and SSAE SOC 2. Disaster recovery plans are documented for backing up and recovering critical systems. Crisis Management procedures are used to direct recovery activities during any significant business disruption and direct communications with key stakeholders, including employees and clients, during major events. Geographic location is taken into consideration during risk assessment and operations to allow effective risk management.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-09	*There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:* *• Identify critical products and services* *• Identify all dependencies, including processes, applications, business partners, and third-party service providers* *• Understand threats to critical products and services* *• Determine impacts resulting from planned or unplanned disruptions and how these vary over time* *• Establish the maximum tolerable period for disruption* *• Establish priorities for recovery* *• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption* *• Estimate the resources required for resumption*	Documented IBM internal policies define requirements and guidelines for performing risk and business impact assessments to identify critical products and services, and dependencies, and define maximum tolerable period for disruption. Business continuity and disaster recovery plans, including recovery point and time objectives, recovery priorities, and resource requirements, are established by each cloud service accordingly and provided as stated in the relevant service description.

Business Continuity Management & Operational Resilience

Control ID in CCM	Control Description	IBM Cloud Services Response
BCR-10	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.*	IBM Cloud services follow a comprehensive set of corporate directives, policies, standards, processes and implementing procedures covering service management and governance to ensure appropriate planning, delivery, and support of IT capabilities supporting IBM's business functions, workforce, and customers. All policies, processes and procedures follow industry best practices from sources such as ISO/IEC 20000, ITIL, and COBIT, fit within the ISO 27001 ISMS framework and follow NIST SP800-53r4 controls. All IBM employees are provided annual training and are required to certify each year that the will comply with IBM policies.
BCR-11	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.*	Data retention policies and procedures are defined and maintained by each cloud service in compliance with IBM corporate directives and records management policies pursuant to its legal, regulatory, statutory, contractual, and business requirements. Cloud service backup and recovery measures are determined and maintained as a part of each cloud service's Business Continuity and Disaster Recovery plan and tested along with all other aspects of the associated plans.

Change Control & Configuration Management

Control ID in CCM	Control Description	Implementation Notes
CCC-01	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.*	The IBM Cloud services ISMS has comprehensive controls used to validate that IBM Cloud services have policies, processes and implementing procedures in place and executed concerning the development or acquisition of all components of IBM cloud services, including operations and actions. The appropriate level of management pre-approves the development and acquisition of new data, physical and virtual applications, infrastructure network, and systems components, corporate, operations, and data center facilities.
CCC-02	*External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).*	The IBM Cloud services ISMS has controls, implemented by the IBM Cloud services, to help maintain consistency in operations up and down the supply chain. IBM requires external business partners involved in development or maintenance of an IBM cloud service, if any, to adhere to same policies and procedures for change management, release, and testing as internal personnel.
CCC-03	*Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.*	IBM Cloud services follow industry standards and best practices, including SDLC and Secure Engineering to implement a well-defined program to help maintain the confidentiality, integrity and availability of information and services to customers. The ISMS organizes and enforces corporate directives and standards requiring IBM Cloud services to document all steps involved in the delivery of services, including quality assurance testing and formal change management. IBM cloud services undergo architecture and code reviews to ensure adherence to IBM policies and secure engineering requirements and are deployed into production following formal change management procedures. Penetration testing and vulnerability scanning is performed prior to production deployment and regularly thereafter.

Change Control & Configuration Management

Control ID in CCM	Control Description	Implementation Notes
CCC-04	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	IBM Cloud services follow corporate directives, standards, and ISMS controls to mitigate the risk of installation of unauthorized software on any IBM IT asset. Change management processes and procedures are in place to ensure any software installation, configuration or other change is pre-approved by appropriate levels of management. Automated security scans and configuration management is performed on all endpoint devices having access to IBM networks and resources, and on cloud service IT infrastructure networks and systems components.
CCC-05	*Policies and procedures shall be established for managing the risks associated with applying changes to:* *• Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations.* *• Infrastructure network and systems components.* *Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.*	Prior to implementation, changes to a Cloud Service, including its systems, networks and underlying components, are documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Cloud Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel. The change management process defined and reviewed by the ISMS includes the requirement for a back-out plan in all cases. Changes are first applied in a staging area where regression tests are run to evaluate the impact of the change. Emergency change procedures are in place to address critical vulnerabilities, threats, or failures affecting the integrity, security, or availability of a cloud service.

Datacenter Security

Control ID in CCM	Control Description	IBM Cloud Services Response
DCS-01	*Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly and assigned ownership by defined roles and responsibilities.*	As part of the IBM Cloud services ISMS, all assets are required to be logged in a central inventory. Required information includes criticality rating, geographic location, and contact information for the business and security owners. Owner and contact information is maintained and verified regularly to maintain accuracy. The information stored, processed or accessed by each system is classified and the level of confidentiality/criticality of the information drives the business criticality value (BCV) of the IT asset. This BCV is also used by Business Continuity and Disaster Recovery planning.
DCS-02	*Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.*	IBM site security includes physical and technical measures to control physical access and is staffed to monitor all means of ingress. All systems and data are required to be within multiple layers of physical security. IBM has 24x7 guards and security staff.
DCS-03	*Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.*	IBM Cloud services depend on automated inventory as an essential step to network connection. Network scanning cross-referenced to inventory acts as a check to validate that only the systems that are approved for connection do so.
DCS-04	*Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.*	IBM requires approval of authorized personnel prior to relocation or transfer of hardware, software or data to an offsite location.
DCS-05	*Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.*	IBM securely sanitizes physical media intended for reuse prior to such reuse, and destroys physical media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

Datacenter Security

Control ID in CCM	Control Description	IBM Cloud Services Response
DCS-06	*Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.*	IBM corporate policies and directives, with which compliance is mandatory for all IBM employees, establish requirements and guidelines for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Entry into IBM facilities requires use of an access badge issued by IBM corporate security. Access to areas storing sensitive information is restricted, monitored, and audited.
DCS-07	*Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.*	Ingress and egress to secure areas is restricted and monitored 24x7x365 by physical access control mechanisms to ensure that only authorized personnel are allowed access, including, but not limited to, security personnel, locked doors requiring use of authorized access badges, and CCTV.
DCS-08	*Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.*	IBM implements controls providing multi-layered security zones. Controls include identifying and authenticating personnel, and monitoring all access, both ingress and egress, in concentric layers to isolate data processing and storage from casual or unauthorized access. Specific controls cover areas such as loading docks or service bays to mitigate the risk of unauthorized access.
DCS-09	*Physical access to information assets and functions by users and support personnel shall be restricted.*	Please refer to responses provided in DCS07 and DCS-08.

Data Security & Information Lifecycle Management

Control ID in CCM	Control Description	IBM Cloud Services Response
DSI-01	*Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.*	Each cloud service is designed to process data to the extent stated in the relevant service description. Per IBM policy, standards and processes, all information is classified by the data owner according to criteria which includes type, value, confidentiality, and criticality.
DSI-02	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.*	Each IBM Cloud service specifies the geographic location(s) of processing and storage in the relevant service description. Data storage and flows are restricted to those geographic locations and the Cloud services' policies, processes and implementing procedures verify adherence to those terms. Client data is not shared with any third parties without the knowledge and consent of the customer**. Any regulatory, statutory or sub-processor requirements are required to be made clear to the customer. **Unless required to do so by law enforcement – see 27018 Annex A.5.1 and A.5.2
DSI-03	*Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.*	IBM Cloud services encrypt all data in transit across public networks using secure protocols, strong ciphers and key strengths, and use reputable certificate authorities' certificates to verify the identity of servers. Services descriptions of IBM cloud services providing electronic commerce capabilities state measures, such as compliance with PCI-DSS, maintained by the service to protect against fraudulent activity and unauthorized disclosure or modification of ecommerce data.
DSI-04	*Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.*	Please refer to response provided for DSI-01.

Data Security & Information Lifecycle Management

Control ID in CCM	Control Description	IBM Cloud Services Response
DSI-05	*Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.*	IBM's policies and standards require that production data not be used for test purposes unless necessary, and then only with customer approval. If customer approval is given to utilize production data in test, then any sensitive, personally identifiable, or customer confidential information contained in the copy intended for transfer into a non-production environment is appropriately protected (e.g. de-identified, anonymized, etc.) prior to transfer. If customer data is transferred into a non-production environment, such as to reproduce an error or incident upon customer request, the data is protected in the non-production environment at least at the level of the production environment, and such data is securely erased prior to re-use of the non-production systems.
DSI-06	*All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.*	IBM enforces that all data is classified and protected according to legal, regulatory, and contractual obligations. All cloud service systems storing, and processing client data have documented business and security owners who are responsible for maintaining such records and classifications and ensuring compliance with associated requirements.
DSI-07	*Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.*	Please refer to response provided for DCS-05.

Encryption & Key Management

Control ID in CCM	Control Description	IBM Cloud Services Response
EKM-01	*Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.*	IBM's Cloud services follow the policy that all encryption keys have an owner or person responsible, or a custodian for customer provided keys. Key management policies are in place and specify the responsibilities for key management.
EKM-02	*Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.*	IBM policies provide requirements and implementation guidelines covering the complete lifecycle and management of cryptographic keys. These policies are reviewed, updated and approved by management on a regular basis. In compliance with IBM policies and implementation guidelines, IBM cloud services that include management of cryptographic keys maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use. Customers will be notified of material changes within the cryptosystem, if any that affect the security of the customer's information.
EKM-03	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.*	IBM corporate policies and directives establish requirements for the use of encryption protocols for protection of sensitive data in storage, data in use, and data in transit per applicable legal, statutory, regulatory compliance, and contractual obligations. Each IBM cloud services encrypts data to the extent provided in the relevant service description.

Encryption & Key Management

Control ID in CCM	Control Description	IBM Cloud Services Response
EKM-04	*Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.*	IBM maintains formal policy requirements and implementation guidelines for the use of encryption to protect information in transit and at rest. This includes the storage, deployment and use of encryption keys. Offering specific documentation specifies the roles and access permissions to keys.

Governance & Risk Management

Control ID in CCM	Control Description	IBM Cloud Services Response
GRM-01	*Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.*	IBM maintains baseline security requirements for all systems and network components that comply with applicable legal, statutory, and regulatory compliance obligations, and utilizes automated configuration management to monitor and enforce adherence to such requirements. Baseline requirements are reviewed and updated regularly. Deviation from security baseline requirements requires approval by authorized personnel. Formal change management procedures are maintained and followed for the performance of production deployment and updates.
GRM-02	*Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:* *• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure* *• Compliance with defined retention periods and end-of-life disposal requirements* *• Data classification and protection from unauthorized use, access, loss, destruction, and falsification*	The IBM Cloud services' ISO/IEC 27001 ISMS is certified and follows risk assessment requirements from ISO/IEC 27005:2011 and other industry-accepted standards. Frequent audits by independent 3rd parties verify that IBM meets all requirements for handling sensitive data, and retaining records and other data, through the lifecycle, including end-of-life disposal.
GRM-03	*Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.*	IBM management is involved in all aspects of the ISMS, meeting or exceeding the requirements in all section 5 clauses of ISO/IEC 27001. All IBM employees are required to complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional policy and process training is provided to persons granted administrative access to Cloud Service components that is specific to their role within IBM's development, operation and support of the Cloud Service, and as required to maintain compliance and certifications stated in the relevant service description.

Governance & Risk Management

Control ID in CCM	Control Description	IBM Cloud Services Response
GRM-04	*An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:* *• Risk management* *• Security policy* *• Organization of information security* *• Asset management* *• Human resources security* *• Physical and environmental security* *• Communications and operations management* *• Access control* *• Information systems acquisition, development, and maintenance*	IBM's Information Security Management System (ISMS) for cloud services is ISO 27001 certified, and the certificate is publicly available at: ISO 27001 ISO Certificate. Areas covered by the ISMS include: • Risk assessment and treatment • Resources and competencies • Information security policies • Organization of information security • Human resource security • Asset management • Identity management and access control • Cryptography • Physical and environmental security • Operations security • Communications security • System acquisition, development and maintenance • Supplier Relationships • Information security incident management • Business continuity management • Compliance with legal, regulatory and contractual obligations • Privacy controls

Governance & Risk Management

Control ID in CCM	Control Description	IBM Cloud Services Response
GRM-05	*Executive and line management shall take formal action to support information security through clearly-documented direction and commitment and shall ensure the action has been assigned.*	IBM maintains extensive corporate directives authorizing and requiring information security activities, including the creation and implementation of standards, processes and procedures. These directives and other corporate policies are reviewed and approved annually. In addition, top level management has authorized, reviewed and approved the ISO ISMS activities, including risk assessment, risk treatment plans, internal and external audits, and many other actions. As a part of those activities, roles and responsibilities are defined and assigned and all plans and actions are tracked to completion. Annual training on cybersecurity and information security areas is required for all employees and completion monitored as part of the terms of employment.
GRM-06	*Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.*	Please refer to responses provided for GRM-04 and GRM-05. In addition, IBM Cloud services follow supply-chain practices indicated in the 27001 A.15 controls to verify suppliers meet the same requirements as IBM itself meets. IBM contractually requires its cloud service sub processors, if any, to maintain technical and organizational security and privacy measures that align with and support IBM's legal, statutory, regulatory compliance, and contractual obligations. . IBM Cloud services, as per multiple controls in ISO/IEC 27017, provide information to the offerings' customers to enable all organizations to provide end-to-end information security.

Governance & Risk Management

Control ID in CCM	Control Description	IBM Cloud Services Response
GRM-07	*A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.*	IBM has terms of employment that enjoin all employees to meet all legal, contractual and ethical obligations. As part of the employment offer package, confidential disclosure agreements (CDAs/NDAs) are signed by all employees. Annual business conduct guidelines training is required of all employees and verifies they are aware of disciplinary action policies.
GRM-08	*Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.*	See GRM-02. As part of its annual reviews of all corporate directives, policies, standards, processes and procedures, IBM reviews changes to the threat landscape in light of ongoing risk assessments. Other events, including new threats and vulnerabilities, may cause this process to be initiated more frequently. Following strict change management practices, appropriate changes and updates are made, reviewed/approved by the appropriate level of executive management and implemented. Supply-chain management enables vendors and contractors to be aware of any changes and verifies they meet the same requirements.
GRM-09	*The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.*	See GRM-08.

Governance & Risk Management

Control ID in CCM	Control Description	IBM Cloud Services Response
GRM-10	*Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).*	IBM Cloud services perform formal risk assessments on at least an annual basis as part of the ISO 27001 certified ISMS. This is in accordance with clauses 6 and 8 of ISO / IEC 27001:2013. Audits and other activities (e.g. KPI testing) help verify that the treatment plans and any corrective actions to address the risk from the assessment are carried out and all changes are factored into ongoing assessments. Executive management is involved in the review of all risk assessments and progress of risk treatment plans.
GRM-11	*Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.*	Identified risks are cataloged and managed in a manner consistent with industry-accepted standards. Risk treatment plans define acceptable mitigation level, resolution time frame, and mitigation roles and responsibilities, and require executive review and approval. IBM cloud service risk management policies and procedures are regularly reviewed and validated in both internal audits and external third-party ISO 27001 certification audits.

Human Resources

Control ID in CCM	Control Description	IBM Cloud Services Response
HRS-01	*Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.*	IBM maintains and follows formal documented policies and procedures for the return of company-owned assets upon termination of employment and expiration of external business relationships.
HRS-02	*Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.*	IBM maintains and follows mandatory employment verification requirements for all new hires. In accordance with IBM internal process and procedures, these requirements are periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.
HRS-03	*Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.*	IBM employment agreements include provisions requiring adherence to IBM information governance and security policies and must be accepted and signed before access is granted to IBM facilities, resources, and assets. Further, all IBM employees are required to complete security and privacy education annually and certify each year that they understand and will comply with IBM's information governance and security policies and Business Conduct Guidelines.
HRS-04	*Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.*	IBM’s HR policies clearly document the roles and responsibilities that the corporation, management and employees have. These roles and responsibilities are clearly communicated, and annual training is tracked and enforced.

Human Resources

Control ID in CCM	Control Description	IBM Cloud Services Response
HRS-05	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).*	IBM's mobile device policy is documented and provided to all employees on the IBM intranet, including limitations to hardware, software, and acceptable use. IBM provides and requires the use of mobile device management software to deploy and maintain required security configuration settings. Mandatory annual training includes a review policy requirements and conditions, including the right of IBM to examine any mobile device provided by IBM, or used to conduct IBM business.
HRS-06	*Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.*	IBM follows industry standard practices, and all legal, regulatory and contractual obligations, in its Confidential Disclosure Agreements (CDAs or NDAs). Requirements for confidentiality agreements reflecting the organization's needs for the protection of data and operational details are identified, documented and reviewed at planned intervals.
HRS-07	*Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.*	Roles and responsibilities of contractors, employees, and third-party users are documented as they relate to information assets and security within IBM information security policies and made available on the IBM intranet. Roles and responsibilities are further addressed in mandatory annual security and privacy training.
HRS-08	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.*	IBM maintains documented policies and procedures defining allowances and conditions for permitting usage of organizationally-owned and managed end-point devices and IT infrastructure network and systems components, including allowances and conditions permitting usage of personal mobile devices and applications with access to corporate resources.

Human Resources

Control ID in CCM	Control Description	IBM Cloud Services Response
HRS-09	*A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.*	IBM mandates annual business conduct and cyber-awareness training for all employees. IBM further requires all contractors, vendors and other onsite personnel to be certified by their employer to have completed the equivalent annual training. Further training and certifications are required for some types of data access (e.g. HIPAA data).
HRS-10	*All personnel shall be made aware of their roles and responsibilities for:* *• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.* *• Maintaining a safe and secure working environment*	All IBM personnel are made aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations, and maintaining a safe and secure working environment, in mandatory annual security, privacy, and business conduct guidelines training.
HRS-11	*Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.*	The ISMS has controls, implemented by the Cloud services, for unattended workspaces, computer screens and other forms of information display to be cleared of any information that may be sensitive. This includes 'screen-savers' that hide what the last user was working on after a short period of time. Papers, hardcopy, media or other possibly sensitive material must be secured in a locked drawer (or equivalent) when not in use.

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-01	*Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.*	Access to audit tools and log information is restricted to personnel with specific, documented, and approved business need. All use of audit tools and information is subject to IBM policies concerning business conduct, terms of employment and non-disclosure agreements. Further, IBM maintains measures protecting such logs against unauthorized access, modification and accidental or deliberate alteration or destruction.

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-02	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:* *• Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)* *• Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)* *• Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))* *• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)* *• Account credential lifecycle management from instantiation through revocation* *• Account credential and/or identity store minimization or re-use when feasible* *• Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)* *• Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions* *• Adherence to applicable legal, statutory, or regulatory compliance requirements*	IBM has extensive controls, which the Cloud services ISMS makes use of, to verify the identity of all personnel. Employees and contractors are validated at least daily against a corporate database for status. Physical access is controlled with picture identity badges with embedded electronic codes. In addition, biometric measures are implemented at IBM Cloud data centers. System to system identification is also used to validate that the access attempts are being initiated from recognized systems. Multi-factor authentication is used when appropriate to provide additional assurance of identity. IBM's Cloud services, following the ISMS requirements, control access and privilege through the use of W3ID which is federated with IBM's internal control mechanisms. Through the use of a Controlled Access System (CAS) and employee identification cards, all physical access can be controlled through the badge readers at all entry/exit portals for IBM sites, buildings, data centers and facilities. Additional biometric security is required for IBM Cloud secure areas. Through the use of IBM internal control and monitoring systems, Cloud services can document, create, group, provision, suspend and revoke access provisions quickly and for some functions automatically. Following the principles of least privilege and segregation of duties (see IAM-05), Cloud services can generate reports to quickly check status, determine any needed actions, and verify access according to contractual, legal and regulatory obligations.

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-03	*User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.*	Access to all APIs, diagnostic functions, and configuration capabilities are restricted with credentials that are in turn linked to identification and access-controlled systems, applications and personnel.
IAM-04	*Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.*	The Cloud service ISMS provides policy requirements, implemented by processes and procedures, and verified by KPI testing and audits, to identify all accesses to all Cloud service infrastructure including all systems and networks resources. All access is mapped to a person responsible and access granted according to their documented levels of permission. In addition, all access and operations are logged in an SIEM where filters and triggers are set to notify the appropriate personnel of any unusual events.
IAM-05	*User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.*	IBM Cloud services are required by IBM to complete a detailed Separation of Duties (SOD) matrix based on roles, tasks and specified personnel, and to verify the access for all individuals in those roles have no conflict of interest. Management must approve this matrix which is kept as an exhibit for both internal and external audits.
IAM-06	*Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.*	Access to the IBM's developed applications, program, and object source code, and other forms of intellectual property, and use of proprietary software is restricted following the rule of least privilege based on job function as provided in responses to IAM-02, IAM-04, and IAM-05.

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-07	*The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.*	The ISMS requires the evaluation of risks that cover these requirements. Policy, process and implementing procedures cover the control over, monitoring of, and impact of any unauthorized or inappropriate access. All appropriate steps are taken before access is provisioned or permissions granted.
IAM-08	*Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.*	The ISMS requires all Cloud services to follow controls aligned with internal IBM information security policies and standards (which in turn are aligned with industry standards and best practices) for all identity management. The internal standards require offerings to follow least privilege principles and to tightly control access to identities, limiting access to such information to personnel with a documented business need-to-know. (See IAM-05 for more information on segregation of duties)
IAM-09	*Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	IBM Cloud services, following the ISMS direction and controls, ensure all access is approved by appropriate authority prior to provisioning. (See IAM-08 and IAM-05 for more information)

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-10	*User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.*	IBM Cloud services are required to conduct Continued Business Need (CBN) reviews on a regular basis which checks for authorization, entitlements, segregation of duties, least privilege, and related. Remediation of issues is required immediately after identification and all review and actions are recorded as auditable evidence. (See IAM-08 and IAM-05 for more information)
IAM-11	*Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	IBM Cloud services, following IBM's policies and standards (see IAM-08), require immediate de-provisioning of access to data and/or systems, equipment and other assets when a user's status changes due to termination of employment or business relationship. For IBM personnel, including supplemental and contract, much of this is automated. Personnel transfer or other changes are controlled with transition plans ending with de-provisioning of access. IBM Cloud services will share this information with authorized customer representatives, as allowed by contractual, legal and regulatory controls, upon request.
IAM-12	*Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:* *• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)* *• Account credential lifecycle management from instantiation through revocation* *• Account credential and/or identity store minimization or re-use when feasible* *• Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)*	IBM Cloud services make available to cloud service customers the ability to permit and/or restrict user account credentials to meet all contractual, regulatory and legal obligations. The requirements for APIs/SSO/Federation/etc. (where applicable), identity/access lifecycle from end to end, identity/credential store minimization, controls on re-use and all elements of industry standards and best practices for authentication, authorization and accounting are part of standard policies and procedures and are implemented as they are applicable.

Identity & Access Management

Control ID in CCM	Control Description	IBM Cloud Services Response
IAM-13	*Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.*	IBM Cloud services have policies, implemented by processes and procedures, requiring and validating that any utility programs of this type are restricted to authorized users and their use logged and monitored. The installation of software that may allow users to override offering controls is also restricted.

Interoperability & Portability

Control ID in CCM	Control Description	IBM Cloud Services Response
IPY-01	*The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.*	IBM Cloud services support the use of industry standard, open-format, APIs as published in each offering's documentation.
IPY-02	*All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).*	IBM Cloud services provide all customer data in mutually agreed upon formats as per standard contract language or by special request. Unless the customer specifies otherwise, standard file formats are used such as .doc, .xls, .pdf, and flat text files.
IPY-03	*Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.*	IBM Cloud services supply well documented API information for ease of application development, usage, support, and information exchange. APIs are implemented using HTTPS over TLS and other secure protocols, REST APIs, JSON, and many other secure methods of interoperable communications.
IPY-04	*The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.*	See IPY-03.
IPY-05	*The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.*	When applicable, IBM Cloud services use documented, industry standard virtualization platforms and formats.

Infrastructure & Virtualization Security

Control ID in CCM	Control Description	IBM Cloud Services Response
IVS-01	*Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.*	IBM Cloud services adhere to a high standard of security, integrity and assurance. The Cloud services ISMS requires the logging to a central location of all activity, coordination of time stamps via a common time source, and all administrative actions are attributable to a unique natural person. Logs are protected from modification and deletion and meet or exceed minimum retention requirements for possible forensic investigation or suspicious activity investigation. Logging and monitoring meets all contractual, legal and regulatory requirements and conforms to industry-accepted practices.
IVS-02	*The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).*	IBM Cloud services based in either virtual machines or containers use baseline images that are carefully managed and updated to maintain a high level of security with all changes following strict change controls, the actual changes logged, and the logs monitored. When those images are deployed, any changes follow the same strict change controls and are logged and monitored as well. The logging and monitoring automation will send alerts to the appropriate personnel if any anomalous activity is detected. Strict controls over the installation and/or use of any unapproved software are in place. Strict change management is followed for any software installation, update or configuration change. Testing of baseline images as well as systems deployed from them is conducted to determine any vulnerabilities or configuration changes. Any discovered vulnerabilities result in an alert being sent to the appropriate personnel. IBM's comprehensive security incident handling process is invoked whenever there is any suspicious activity or attempt to compromise cloud service systems or networks.

Infrastructure & Virtualization Security

Control ID in CCM	Control Description	IBM Cloud Services Response
IVS-03	*A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.*	As a basic part of the Cloud services ISMS controls, IBM's Cloud services synchronize clocks to facilitate analysis of logging information. The same requirement is passed down the supply chain to enable multi-service analysis.
IVS-04	*The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.*	IBM cloud services, following the ISMS, monitor and measure capacity of resources and use that data gathered to implement any indicated changes to help maintain agreed upon levels of service. The same requirements are passed down the supply chain to any suppliers or providers of service.
IVS-05	*Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).*	The ISMS requires IBM cloud services to be aware of the supply chain impacts of security. Suppliers or providers of service are selected on the basis of meeting vulnerability assessments and testing helps verify all parties are meeting expectations.
IVS-06	*Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.*	The ISMS requires IBM Cloud services to implement security and privacy controls when designing networks, physical or virtual, and when deciding how physical or virtual systems populate network security zones. All originating end-points, the protocols used, the traversal of security zones and the terminating end-points are part of the network control documentation which is reviewed and updated whenever any changes are implemented as part of the standard planning process, which includes the initialization of network services. All network traffic is monitored at the control points for the security zones and logged to a central SIEM for analysis and monitoring. Alerts are generated for any suspicious activity. Access to any internal system or device and any actions taken on those systems or devices are also logged.
IVS-07	*Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and*	IBM Cloud services' ISMS defines requirements for establishment of services and initialization of network service which include the hardening of systems and

Infrastructure & Virtualization Security

Control ID in CCM	Control Description	IBM Cloud Services Response
	logging as part of their baseline operating build standard or template.	networks, protection from malware, logging of all activity and other integrity controls. After deploying a system or container from the baseline template or image, security testing is done to confirm that the integrity of the system is maintained, and any redeployment is made from a baseline configuration that is up to date and includes all hardening measures. (See IVS-02 for more information)
IVS-08	*Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.*	The IBM requires all IBM Cloud services' production systems to be segregated from any test systems, not only physically, but logically, including strict access controls and segregation of duties. (See IVS-06 for more information)
IVS-09	*Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:* *• Established policies and procedures* *• Isolation of business-critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance* *• Compliance with legal, statutory, and regulatory compliance obligations*	IBM Cloud services employ a variety of methods to segregate user access. Design of network infrastructure includes the ISMS requirements to provide a defense in depth and identity/access management is used to control who is allowed access to what at the boundaries. Higher levels of identity/access management is required for business critical assets including sensitive data and the Cloud services add extra layers of control on top of the foundation provided by design. IBM Cloud services comply with all contractual, legal and regulatory obligations. (See IVS-06 for more information)
IVS-10	*Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.*	All IBM Cloud services use encrypted network protocols when installing or migrating systems, applications or transferring data. In most cases, a segregated network is used for such system management operations.

Infrastructure & Virtualization Security

Control ID in CCM	Control Description	IBM Cloud Services Response
		Security validation testing is used to validate that no unencrypted channels are available on production systems and equipment.
IVS-11	*Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).*	All access to any hypervisor administrative, configuration or management consoles, functions and APIs is restricted, on a least privilege basis, to personnel with a business need. All access and operations performed are logged and monitored. (See IAM-03 for more information)
IVS-12	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:* *• Perimeter firewalls implemented and configured to restrict unauthorized traffic* *• Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)* *• User access to wireless network devices restricted to authorized personnel* *• The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network*	IBM has policies and controls over access to IBM owned or managed wireless networks that include requirements on what may be used to connect, who may connect, identification of each device and person, what may be connected to (destination end-points), and the use of strong encryption and secure protocols for all wireless connections. IBM controls include – restrictions on the type/version of any wireless device, requiring special software be installed on any wireless device that connects to any IBM network, special configuration for such wireless devices that include encryption keys, protocol settings and disabling of any applications / software not specifically permitted. However, unless a Cloud service specifically involves support for wireless connections, Cloud services do not allow any wireless connections and require wireless interfaces to be disabled on the offering's systems and equipment. Random sweeps are made for rogue wireless network devices and corrective actions will be taken immediately if such are found.
IVS-13	*Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth*	IBM Cloud services maintain network diagrams as part of the ISMS network control documentation. The diagrams include classification of information processes, identification of critical dataflows (including

Infrastructure & Virtualization Security

Control ID in CCM	Control Description	IBM Cloud Services Response
	techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	high-risk) and a table of network connections, protocols and end-points. This allows the offering to implement defense in depth and other measures to maintain the confidentiality and integrity of all information in transit. Technical vulnerability testing provides objective means to measure the effectiveness.

Mobile Security

Control ID in CCM	Control Description	IBM Cloud Services Response
MOS-01	*Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.*	See IVS-12 for information on general use of mobile devices. Required annual training for business conduct and cyber-security document all personnel are aware of these requirements.
MOS-02	*A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.*	See IVS-12 for information on general use of mobile devices. IBM requires that only IBM approved applications be installed on mobile devices accessing or connecting to wireless networks owned or managed by IBM.
MOS-03	*The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.*	See IVS-12 for information on general use of mobile devices. IBM internal standards specify requirements in this area.
MOS-04	*The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.*	See IVS-12 for information on general use of mobile devices. Terms of employment and IBM internal standards cover BYOD.
MOS-05	*The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.*	See IVS-12 for information on general use of mobile devices. Required annual training for business conduct and cyber-security document all personnel are aware of these requirements.
MOS-06	*All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.*	See IVS-12 for information on general use of mobile devices.
MOS-07	*The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.*	See IVS-12 for information on general use of mobile devices. Required annual training for business conduct and cyber-security document all personnel are aware of these requirements.

Mobile Security

Control ID in CCM	Control Description	IBM Cloud Services Response
MOS-08	*The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.*	See IVS-12 for information on general use of mobile devices. Required annual training for business conduct and cyber-security document all personnel are aware of these requirements.
MOS-09	*An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.*	See IVS-12 for information on general use of mobile devices. IBM has internal standards that require all mobile devices, regardless of ownership, to register and install specific management software. The process is well documented and is part of the required annual training. This is part of the terms of employment.
MOS-10	*A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.*	See MOS-09 above.
MOS-11	*The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.*	See IVS-12 for information on general use of mobile devices and MOS-09 for device management. Strong encryption and secure protocols are required for all communications.
MOS-12	*The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).*	See IVS-12 for information on general use of mobile devices and MOS-09 for device management. IBM has specific requirements prohibiting jailbreaking or rooting mobile devices and the central management software is designed to detect and report any instance.
MOS-13	*The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.*	See IVS-12 for information on general use of mobile devices and MOS-09 for device management. IBM has specific language that any device connecting to IBM's networks or used to conduct IBM business is in-scope and subject to all the controls listed in IBM's internal standards. This is part of the terms of employment.

Mobile Security

Control ID in CCM	Control Description	IBM Cloud Services Response
MOS-14	*BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.*	These requirements are part of IBM's standards, communicated via annual business conduct guidelines and cyber-security training. For mobile devices, the central management software detects and enforces these requirements.
MOS-15	*Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.*	All mobile devices used to conduct IBM business or connecting to IBM's networks are required to use the mobile device management software which enforces this requirement.
MOS-16	*Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.*	See MOS-15.
MOS-17	*The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).*	See MOS-15.
MOS-18	*All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.*	See MOS-15.
MOS-19	*Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.*	See MOS-15.
MOS-20	*The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.*	See IVS-12 for information on general use of mobile devices.

Security Incident Management, E-Discovery & Cloud Forensics

Control ID in CCM	Control Description	IBM Cloud Services Response
SEF-01	*Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.*	IBM has a comprehensive program to handle any information security incident, confirmed or suspected and designated personnel to contact via well-communicated channels. Physical security at all IBM sites is manned 24x7 and is also able to quickly connect with emergency services, including law enforcement. IBM has dedicated groups to serve as the points of contact with all regulatory authorities.
SEF-02	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.*	IBM Computer Security Incident Response Team (CSIRT) is well trained and has internal technical and organizational measures (TOMs) that include triage, preservation of evidence, chain of custody, response time windows and executive management involvement.
SEF-03	*Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.*	IBM has internal policies and standards that cover these requirements including clearly defined channels for reporting of information security events. The required annual training for all personnel reviews the policies, processes, and procedures. Information security events are handled according to industry best practices and conform to all contractual, regulatory and legal requirements.
SEF-04	*Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.*	Once an information security incident, confirmed or suspected, is reported to the CSIRT, clear direction is given to the reporter, who is required by policy and terms of employment to follow those directions. (See SEF-01 and SEF-02)
SEF-05	*Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.*	Monitoring and metrics are part of the information security incident management procedures. Executive management is kept informed and is involved in all planning and the decision-making process

Supply Chain Management, Transparency and Accountability

Control ID in CCM	Control Description	IBM Cloud Services Response
STA-01	*Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.*	The IBM Cloud services ISMS documents the requirements in many areas to manage data security risks. Controls include extensive segregation of duties, role-based access controls based on least privilege principles. All suppliers and providers of service are contractually required to adhere to the same high standards.
STA-02	*The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).*	IBM makes vulnerability information publicly available and promptly notifies customers of the offering of any incident involving that customer's data. Other entities in the supply chain are notified as required and according to contractual, regulatory and legal obligations.
STA-03	*Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.*	IBM follows industry standard best practices and complies with all contractual obligations to document APIs and clearly communicates them with customers. Service Level Agreements (SLAs) and capacity expectations capture offering expectations, policies and procedures.

Supply Chain Management, Transparency and Accountability

Control ID in CCM	Control Description	IBM Cloud Services Response
STA-04	*The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.*	IBM has multiple programs to assess the effectiveness of policy, standards, processes and procedures. Many technical measures have monthly policy updates to maintain currency with the evolving information security landscape. All requirements are also applicable to the supply chain and compliance is monitored. As part of IBM's programs, the Cloud services ISMS conducts quarterly KPI testing, semi-annual internal audits and external surveillance audits. The results of all measures and metrics, as well as the audit reports and any findings are reviewed with executive management, and appropriate measures taken to constantly improve performance and to meet legal, regulatory and contractual obligations.

Supply Chain Management, Transparency and Accountability

Control ID in CCM	Control Description	IBM Cloud Services Response
STA-05	*Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:* *• Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)* *• Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships* *• Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts* *• Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)* *• Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed* *• Expiration of the business relationship and treatment of customer (tenant) data impacted* *• Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence*	The ISMS supplier management controls, coupled with IBM's standard global procurement process, helps maintain that all vendors, contractors and suppliers of services are vetted, sign binding non-disclosure agreements that meet the requirements (see HRS-06) and require adherence to all technical and organizational measures (TOMs), and security requirements. IBM's legal teams review and approve all contractual documents, including: • Supplier and Customer Contracts, • Service Descriptions (SDs), • Service Level Agreements (SLAs) • and the IBM Cloud » Cloud Services Agreement, » Data Security & Privacy Principles, » Data Processing Addendum (w/ EU Standard Contractual Clauses) ** See introduction section for links and other information.

Supply Chain Management, Transparency and Accountability

Control ID in CCM	Control Description	IBM Cloud Services Response
STA-06	*Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.*	IBM Cloud services, as required by the ISMS, exercise due diligence in reviewing suppliers' and partners' certifications (e.g. ISO 27001/17/18), statements of applicability (SOA) and attestations (e.g. SSAE16 / ISAE3402) and account for any risks to the Cloud service or customers that may be inherited.
STA-07	*Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.*	This control is covered as a standard part of the Cloud services ISMS. Reviews and audits are performed at least annually, and appropriate corrective actions taken for any non-conformities (if any) found.
STA-08	*Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.*	This control is covered as a standard part of the Cloud services ISMS. (See STA-04, -05, -06 and -07 above)
STA-09	*Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.*	This control is covered as a standard part of the Cloud services ISMS. (See STA-04, -05, -06 and -07 above)

Threat & Vulnerability Management

Control ID in CCM	Control Description	IBM Cloud Services Response
TVM-01	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	As part of IBM's standard end-point management policy, processes and procedures, standard images which include malware detection and prevention software and/or controls, are deployed on all IBM owned devices as well as BYOD used to conduct IBM's business or that of IBM's customers. Networking devices use common rulesets and configurations whenever possible and strict change management controls any software or configuration changes. (See CCC-04, IVS-02, IVS-07 & MOS-01)

Threat & Vulnerability Management

Control ID in CCM	Control Description	IBM Cloud Services Response
TVM-02	*Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.*	IBM internal standards and procedures, as well as the Cloud services ISMS, require weekly network vulnerability scanning with daily updates to the tests and a monthly policy review/update so that testing continues to stay current with the evolving threat landscape. IBM internal standards also reference IBM's Security, Asset & Risk Management (SARM) which provides security advisory alerts and information and includes the due-dates for response. Cloud services make use of end-point management tools to monitor all parts of the offering's infrastructure which validates timely application of security updates. Both network vulnerability detection and security advisory management include prioritization according to industry standard risk assessment, which is further prioritized according to the needs of the offerings' business needs. Changes to Cloud service systems and software are handled according to strict change management which produces auditable exhibits. Quarterly internal penetration testing (PenTesting) is performed and annual external (3rd party) PenTests are also required. PenTest reports are reviewed with appropriate levels of offering management and remediation to closure is carefully tracked. Information on these processes is available upon client request.

Threat & Vulnerability Management

Control ID in CCM	Control Description	IBM Cloud Services Response
TVM-03	*Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.*	Software used by IBM Cloud services is reviewed and carefully selected in accordance with all defined security objectives. Mobile code is not used in IBM Cloud services. IBM has strict policies, processes and implementing procedures concerning the use by personnel of end-point devices (workstations, laptops, mobile devices, etc.) and those policies are enforced by end-point management tools which are required to be installed on all such devices.

CAIQv3.0.1 NS

Version	Control ID
3.0.1-09-16-2014	N/A
3.0.1-11-24-2015	MOS-02
3.0.1-11-24-2015	MOS-04
3.0.1-11-24-2015	MOS-05
3.0.1-11-24-2015	MOS-10
3.0.1-11-24-2015	MOS-12
3.0.1-11-24-2015	MOS-14
3.0.1-11-24-2015	MOS-16
3.0.1-11-24-2015	MOS-17
3.0.1-11-24-2015	SEF-01
3.0.1-11-24-2015	AAC-02
3.0.1-11-24-2015	AAC-02
3.0.1-11-24-2015	CCC-04
3.0.1-11-24-2015	DSI-01
3.0.1-11-24-2015	DSI-01
3.0.1-11-24-2015	DSI-04
3.0.1-11-24-2015	DSI-04
3.0.1-11-24-2015	DSI-05
3.0.1-11-24-2015	DSI-05
3.0.1-11-24-2015	DSI-06
3.0.1-11-24-2015	GRM-04
3.0.1-11-24-2015	GRM-08
3.0.1-11-24-2015	HRS-09
3.0.1-11-24-2015	HRS-10
3.0.1-11-24-2015	IAM-05
3.0.1-11-24-2015	IAM-12
3.0.1-11-24-2015	IVS-11
3.0.1-11-24-2015	HRS-05
3.0.1-11-24-2015	IVS-10
3.0.1-11-24-2015	BCR-03
3.0.1-11-24-2015	DSI-03
3.0.1-11-24-2015	DSI-03
3.0.1-11-24-2015	DSI-03
3.0.1-11-24-2015	DSI-04
3.0.1-11-24-2015	DSI-04
3.0.1-11-24-2015	GRM-10
3.0.1-11-24-2015	GRM-11
3.0.1-11-24-2015	GRM-08
3.0.1-11-24-2015	IAM-07
3.0.1-11-24-2015	AIS-01
3.0.1-11-24-2015	IVS-01
3.0.1-11-24-2015	IVS-07
3.0.1-11-24-2015	TVM-02
3.0.1-11-24-2015	TVM-03
3.0.1-11-24-2015	AAC-01

3.0.1-11-24-2015	AAC-02
3.0.1-11-24-2015	CCC-05
3.0.1-11-24-2015	DSI-01
3.0.1-11-24-2015	DSI-04
3.0.1-11-24-2015	DSI-05
3.0.1-11-24-2015	DSI-06
3.0.1-11-24-2015	GRM-01
3.0.1-11-24-2015	IAM-07
3.0.1-11-24-2015	SEF-02
3.0.1-11-24-2015	SEF-03
3.0.1-11-24-2015	SEF-04
3.0.1-11-24-2015	AIS-04
3.0.1-11-24-2015	AAC-03
3.0.1-11-24-2015	CCC-03
3.0.1-11-24-2015	HRS-03
3.0.1-11-24-2015	HRS-04
3.0.1-11-24-2015	HRS-05
3.0.1-11-24-2015	HRS-07
3.0.1-11-24-2015	HRS-08
3.0.1-11-24-2015	STA-06
3.0.1-11-24-2015	EKM-04
3.0.1-11-24-2015	CCC-02
3.0.1-11-24-2015	CCC-03
3.0.1-11-24-2015	IVS-02
3.0.1-11-24-2015	IVS-05
3.0.1-11-24-2015	MOS-12
3.0.1-11-24-2015	STA-02
3.0.1-11-24-2015	TVM-02
3.0.1-11-24-2015	AIS-04
3.0.1-11-24-2015	BCR-08
3.0.1-11-24-2015	BCR-08
3.0.1-11-24-2015	BCR-10
3.0.1-11-24-2015	CCC-01
3.0.1-11-24-2015	CCC-05
3.0.1-11-24-2015	GRM-01
3.0.1-11-24-2015	IAM-02
3.0.1-11-24-2015	IAM-09
3.0.1-11-24-2015	IVS-09
3.0.1-11-24-2015	IPY-02
3.0.1-11-24-2015	IPY-02
3.0.1-11-24-2015	MOS-11
3.0.1-11-24-2015	N/A
3.0.1-02-01-2016	AIS-02
3.0.1-02-01-2016	AAC-03
3.0.1-02-01-2016	BCR-02
3.0.1-02-01-2016	BCR-03
3.0.1-02-01-2016	CCC-01
3.0.1-02-01-2016	CCC-03
3.0.1-02-01-2016	DSI-06
3.0.1-02-01-2016	DCS-02
3.0.1-02-01-2016	DCS-04

3.0.1-02-01-2016	DCS-05
3.0.1-02-01-2016	DCS-06
3.0.1-02-01-2016	EKM-03
3.0.1-02-01-2016	GRM-01
3.0.1-02-01-2016	GRM-04
3.0.1-02-01-2016	GRM-06
3.0.1-02-01-2016	GRM-08
3.0.1-02-01-2016	HRS-02
3.0.1-02-01-2016	HRS-04
3.0.1-02-01-2016	HRS-05
3.0.1-02-01-2016	HRS-06
3.0.1-02-01-2016	HRS-08
3.0.1-02-01-2016	HRS-09
3.0.1-02-01-2016	HRS-10
3.0.1-02-01-2016	IAM-01
3.0.1-02-01-2016	IAM-02
3.0.1-02-01-2016	IAM-06
3.0.1-02-01-2016	IAM-07
3.0.1-02-01-2016	IAM-09
3.0.1-02-01-2016	IAM-11
3.0.1-02-01-2016	IAM-12
3.0.1-02-01-2016	IAM-13
3.0.1-02-01-2016	IVS-01
3.0.1-02-01-2016	IVS-04
3.0.1-02-01-2016	IVS-06
3.0.1-02-01-2016	IVS-07
3.0.1-02-01-2016	IVS-08
3.0.1-02-01-2016	IVS-09
3.0.1-02-01-2016	IVS-10
3.0.1-02-01-2016	IVS-12
3.0.1-02-01-2016	IPY-01
3.0.1-02-01-2016	IPY-02
3.0.1-02-01-2016	IPY-05
3.0.1-02-01-2016	MOS-01
3.0.1-02-01-2016	MOS-02
3.0.1-02-01-2016	MOS-03
3.0.1-02-01-2016	MOS-04
3.0.1-02-01-2016	MOS-05
3.0.1-02-01-2016	MOS-06
3.0.1-02-01-2016	MOS-07
3.0.1-02-01-2016	MOS-08
3.0.1-02-01-2016	MOS-09
3.0.1-02-01-2016	MOS-10
3.0.1-02-01-2016	MOS-11
3.0.1-02-01-2016	MOS-13
3.0.1-02-01-2016	MOS-14
3.0.1-02-01-2016	MOS-15
3.0.1-02-01-2016	SEF-01
3.0.1-02-01-2016	SEF-02
3.0.1-02-01-2016	SEF-03

3.0.1-02-01-2016	SEF-04
3.0.1-02-01-2016	SEF-05
3.0.1-02-01-2016	STA-01
3.0.1-02-01-2016	STA-02
3.0.1-02-01-2016	STA-03
3.0.1-02-01-2016	STA-04
3.0.1-02-01-2016	STA-05
3.0.1-02-01-2016	STA-06
3.0.1-02-01-2016	STA-07
3.0.1-02-01-2016	STA-08
3.0.1-02-01-2016	STA-09
3.0.1-02-01-2016	TVM-01
3.0.1-02-01-2016	TVM-02
3.0.1-02-01-2016	N/A
3.0.1-02-01-2016	N/A
3.0.1-02-01-2016	N/A
3.0.1-02-01-2016	N/A
3.0.1-10-06-2016	N/A
3.0.1-10-06-2016	N/A
3.0.1-10-06-2016	N/A
3.0.1-09-01-2017	N/A
3.0.1-09-01-2017	N/A
3.0.1-09-01-2017	N/A
3.0.1-09-01-2017	N/A
3.0.1-09-01-2017	N/A

SENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 3.0.1 Change Log

Decription of Changes
Version 3.0.1-09-16-2014 name updated to Version 3.0.1-11-24-2015
Spelling of security
Spelling of security
Spelling of security
Spelling of services
Spelling of services
Spelling of services
Spelling of services
Spelling of security
Spelling of chapter
Spelling of domain
Hyphenation of third-party
Spelling of management
Spelling of personally
Spelling of identifiable
Spelling of personally
Spelling of identifiable
Spelling of personally
Spelling of identifiable
Spelling of stewardship
Spelling of capability
Spelling of domain
Spelling of chapter
Spelling of chapter
Spelling of segregation
Spelling of security
Spelling of management
Spelling of services
Removal of vMotion
Punctuation of telecommunications, and
Style of E-commerce
Spelling of procedures
Spelling of policies
Spelling of procedures
Spelling of policies
Spelling of confidentiality
Spelling of confidentiality
Spelling of chapter
Spelling of confidentiality
Spelling of security
Spelling of lifecycle
Spelling of controls
Spelling of identified
Spelling of vulnerability
Removal of extra space behind .

Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Removal of extra space behind .
Italicized Data Security / Integrity
Italicized Information System
Italicized Quality Testing
Italicized Employment
Italicized Employment
Italicized Mobile Device
Italicized Roles
Italicized Technology
Italicized Supply Chain
Comma after i.e.
Comma after e.g.
Comma after e.g.
Comma after e.g.
Comma after e.g.
Comma after e.g.
Comma after e.g.
Comma after e.g.
Addition of commas
Removed capitalization from Business Impact Assessment
Added period to end of sentence
Addition of commas
Addition of commas
Removal of extraneous space
Addition of commas
Removal of extraneous space
Addition of commas
Addition of commas
Removal of extraneous space
Added period to end of sentence
Addition of commas
Version 3.0.1-11-24-2015 name updated to Version 3.0.1-02-01-2016
Addition of commas
Syntax update (*the capability)
Syntax update (*testing)
Data center changed to two words
Data center changed to two words and addition of comma
Syntax update (*Organizations) and added period to end of sentence
Addition of commas
Addition of commas
Punctuation update of moving question mark to end of sentence

Capitalized Equipment in Control Group title
Addition of commas
Addition of commas
Syntax update (removed *and established, added *the and pluralized needs) and addition of commas
Syntax update (*at)
Addition of commas
Addition of commas
Addition of commas
Addition of commas
Addition of commas
Hyphenation of Non-Disclosure in Control Group title
Syntax update (*remove or and added e.g.)
Addition of commas
Addition of commas
Punctuation update of moving question mark to end of sentence and addition of comma and e.g.
Addition of commas
Addition of commas
Syntax update (*provide)
Addition of commas and fix of typo to you
Addition of commas
Addtion of e.g.,
Syntax update (*the)
Addition of commas
Addtion of e.g., and commas
Punctuation update of new sentence starting with *These configurations… and deletion of *and before ports.
Replaced i.e. with e.g., and addition of commas
Hyphenation of Non-Production
Addition of commas
Addition of commas
Punctuation update of moving question mark to end of sentence
Updated CID for consistency with a .1
Updated CID for consistency with a .1
Punctuation update of removing extraneous period from e.g.
Updated CID for consistency with a .1
Updated CID for consistency with a .1
Syntax update (*can) and updated CID for consistency with a .1
Updated CID for consistency with a .1
Updated CID for consistency with a .1
Updated CID for consistency with a .1
Addition of commas and updated CID for consistency with a .1
Updated CID for consistency with a .1
Addtion of e.g., and updating to operating system and updated CID for consistency with a .1
Updated CID for consistency with a .1
Updated CID for consistency with a .1
Syntax update (*that) and addition of commas
Updated CID for consistency with a .1
Addition of commas and updated CID for consistency with a .1
Addition of comma
Addition of comma
Addition of e.g., and comma

Addition of comma
Addition of comma
Addition of comma
Addition of comma
Addition of comma
Addition of comma
Addition of comma
Addition of comma
Syntax update (*shall and identify) and addition of comma
Addition of comma and updated CID for consistency with 08.2
Addition of comma
Addition of comma
Addition of comma
Updated column title in A for consistency with CCM v3.0.1 by changing to Control Domain from Control Group
Updated column title in B for consistency with CCM v3.0.1 by changing to Control ID from CGID
Updated column title in C for consistency with CCM v3.0.1 by changing to Question ID from CID
Version 3.0.1-02-01-2016 name updated to Version 3.0.1-10-06-2016
Updated Logo in Change Log Tab (from CCM to CAIQ)
Uopdated Change Log Columns to correct accurate Version Updates
Version 3.0.1-10-06-2016 name updated to Version 3.0.1-12-05-2016
Added HITRUST CSF v8.1
Added PCI DSS v3.2
Added Shared Assessments 2017 AUP
Added CIS-AWS Foundation 1.1
Added NZISM v2.5

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			IBM Cloud IaaS Response
					Yes	No	Not Applicable	
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	x			The IBM Cloud IaaS system development lifecycle is built on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. Including best practices of rule implementation for the development of software and systems, formal change control, utilization of test environments to conduct rigorous testing prior to release. NIST 800-53 control group SC ISO27001 A.14
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	x			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	x			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			x	IBM Cloud IaaS does not outsource software development.
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?			x	
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices and the Physical and Environmental Protection Policy. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 control group CA
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	x			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	x			IBM Cloud IaaS restricts access to information and application system functions in accordance to the NIST 800-53 standard with the Logical Access Control Policy and related procedures. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 control group SI
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	x			IBM Cloud IaaS's Data Security Architecture is designed using industry standards and best practices, NIST 800-53.
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	x			IBM Cloud IaaS works with independent auditors and third-party organizations to meet the industry's most stringent guidelines and to provide the customer certain reports and certificates that they can leverage in their compliance efforts. For a full list of IBM Cloud IaaS Security Compliance Standards visit here: http://www.softlayer.com/compliance To maintain IBM Cloud IaaS's strict security requirements and for the security of all customers IBM Cloud IaaS releases only reports that do not contain security documentation which is proprietary and confidential.
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	x			IBM Cloud IaaS customers as well as perspective customers can download and view the ISO27001 certificate here: http://www.softlayer.com/sites/default/files/assets/page/softlayer_iso27001_2016.pdf IBM Cloud IaaS customers can download the current SOC2 report from the customer portal or contact the IBM Cloud IaaS sales team. The IBM Cloud IaaS Security Operations Center routinely scans internal and external facing non-customer apps for vulnerabilities. The Security Operations Center reports discovered vulnerabilities to the appropriate system owners for remediation in accordance with all applicable standards. IBM Cloud IaaS engages third party groups as well as IBM to conduct penetration testing as prescribed by industry best practices. IBM Cloud IaaS cannot risk the security of systems and all customers by releasing the results of penetration tests however customers should leverage IBM Cloud IaaS's third party certifications as external auditors do review samples of penetration testing. Additionally, IBM Cloud IaaS undergoes Key Control Objective internal audit on a quarterly basis. KCO audits are conducted by an independent 3rd party auditing firm over all IBM Cloud IaaS's core controls which are based on the NIST 800-53 framework. The results from these quarterly audits are reported up through SoftLayer to IBM.
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	x			
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	x			
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	x			
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	x			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?		x		
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	x			
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	x			
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	x			IBM Cloud IaaSemploys logical segmentation in all networks and the hypervisors enforce compute isolation in Virtual Machines. These controls are tested regularly by penetration tests. IBM Cloud IaaS does not touch the tenant's data, but strongly encourages all customers to use encryption mechanisms for data at rest and in transit.
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	x			IBM Cloud IaaS encourages all customers to maintain backups of their data, allowing them to use any backup service provider they choose. IBM Cloud IaaS offers turnkey Evault and R1Soft automatic backup solutions, as well as the ability for customers to create and customize their own backup solution using IBM Cloud IaaS virtual or bare metal server to run a private backup application. To find more out about IBM Cloud IaaS Backup options visit us here http://www.softlayer.com/backup
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	x			IBM Cloud IaaS has datacenters all over the globe, during the ordering process the customer has the ability to select the data center in which they would like their solution to be deployed. IBM Cloud IaaS will not touch or move customers' data without first notifying the customer, unless required by law.
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	x			IBM and IBM Cloud IaaS constantly monitor changing regulatory requirements and subscribe to sources for additional updates. Any changes to the regulatory environment are reviewed and addressed accordingly.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and	Do you provide tenants with geographically resilient hosting options?	x			IBM Cloud IaaS encourages customers to take advantage of IBM Cloud IaaS's extensive network of 40 data centers around the globe to accomplish geographic resiliency. Customers can do this by purchasing instances in as many different locations as desired.
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?	x			IBM Cloud IaaS allows the customer to design and implement failover capability to their select compliance standards.
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	x			IBM Cloud IaaS business continuity plans and processes are designed and maintained in accordance to NIST 800-53 and ISO27001. The business continuity processes are tested internally and as part of our third party audits including by not limited to FedRAMP, ISO27001, PCI, SOC, HIPAA. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 Control Group CP ISO27001 A.17
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	x			IBM Cloud IaaS customers have the option to designate the data center in which their solution will be deployed. IBM Cloud IaaS does not touch or move customers' data without first notifying the customer, unless required by law. IBM Cloud IaaS customers are running over a dedicated Dense Wavelength Division Multiplexing link, and have the ability to utilize documentation provided by IBM Cloud IaaS to recreate the transport route of their data. Understanding the IBM Cloud IaaS network including FCR/BCR and FAS/BAS API customers can view their route into and within a data center. IBM Cloud IaaS cannot tell customers which of our interDC network pipes they are riding across as IBM Cloud IaaS is constantly managing these to ensure enough bandwidth.
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?		x		IBM Cloud IaaS describes how data is transported but does not specify through which legal jurisdictions. IBM Cloud IaaS Customers should take legal jurisdictions into account when designing and deploying their systems across multiple datacenters. IBM Cloud IaaS network routes are detailed on the webpage for further consideration.
Business Continuity Management & Operational Resilience *Documentation*	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	x			IBM Cloud IaaS has extensive documentation on the information system, this documentation is available but restricted to authorized personnel through the IBM Cloud IaaS shared drive. This information is also distributed through training where applicable.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	x			IBM Cloud IaaS's Physical and Environmental Protection controls are in place in all data centers and are validated frequently through internal audits and by independent auditors. NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	x			
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	x			IBM Cloud IaaS has many virtual machine management products and tools available to customers for purchase. IBM Cloud IaaS's offering Flex Images allows customers to capture imagines not only on virtual machines but also on bare metal servers, store them in a single image library, and then these images can be deployed on either kind of system. More about Flex Image can be found here: http://knowledgelayer.softlayer.com/faqs/5#252
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	x			
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	x			IBM Cloud IaaS provides Image Templates as a method to capture an image of a device in order to quickly replicate its configuration with minimal manipulations in the order process. This also allows customers to bring their own image to their IBM Cloud IaaS solution, or visa versa. More about Image Import/Export here: http://knowledgelayer.softlayer.com/topic/image-templates
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	x			
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	x			
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	x			IBM Cloud IaaS's Physical and Environmental Protection controls are in place in all data centers. These controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Cloud IaaS SOC reports provide additional insight the security mechanisms implemented to protect against outages. The SOC3 report is available to customers and perspective customers here: http://static.softlayer.com/sites/default/files/assets/page/softlayer-soc_3-103115.pdf The SOC2 report is available to customers and can be requested via the customer portal or by contacting the IBM Cloud IaaS sales team. NIST 800-53 control group PE ISO27001 A.11
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	x			Every IBM Cloud IaaS server comes with standard monitoring resources at no additional cost. This allows customers to access reports to evaluate their cloud infrastructure performance at any time. For customers with more involved monitoring needs, IBM Cloud IaaS offers several additional options to meet advanced monitoring and reporting needs for greater awareness and visibility. More about monitoring and reporting here: http://www.softlayer.com/server-monitoring IBM Cloud IaaS's SLA can be viewed and downloaded here: https://www.softlayer.com/sites/default/files/sla.pdf
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	x			
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	x			Customers can utilize information and tools provided, including tickets, and the API to determine SLA performance.
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	x			IBM Cloud IaaS maintains a comprehensive portfolio of Policies and Procedures mapped to the NIST 800-53 framework, HIPAA, ISO27001, ISO27017, ISO27018 and the PCI DSS requirements. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?			x	IBM Cloud IaaS does not handle customer's data. Customers are responsible to manage their data retention to the requirements they see fit. IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud IaaS service agreement can be found here: http://static.softlayer.com/sites/default/files/assets/page/softlayer_msa.pdf
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	x			Customer security including customer privacy is one of IBM Cloud IaaS's primary concerns. IBM Cloud IaaS maintains internal procedures and processes pertaining to document requests from law enforcement agencies and how to properly vet these kinds of requests. IBM Cloud IaaS will notify the customer of these kinds of requests or submissions if allowed. Pursuant of the terms of the IBM Cloud IaaS MSA, IBM Cloud IaaS will respond to valid subpoenas or court orders from entities who have proper subpoena power and jurisdiction. If IBM Cloud IaaS believes orders are lacking solid basis More about subpoenas here: http://www.softlayer.com/subpoenas
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	x			IBM Cloud IaaS employs an active active replication allowing resumption of services in near real-time with no data loss. IBM Cloud IaaS backup and redundancy mechanisms are tested at a frequency that aligns with NIST 800-53 and ISO27001 standards. NIST 800-53 Control group CP ISO27001 A12.3
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	x			
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	x			IBM Cloud IaaS maintains a comprehensive portfolio of Policies and Procedures mapped to the NIST 800-53 framework, HIPAA, ISO27001, ISO27017, ISO27018 and the PCI DSS requirements. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 control group SA
		CCC-01.2		Is documentation available that describes the installation, configuration, and use of products/services/features?	x			IBM Cloud IaaS provides detailed guides on installation, configuration, and use of IBM Cloud IaaS services available at knowledgelayer.softlayer.com.
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	x			IBM Cloud IaaS's development security controls that are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Cloud IaaS does not outsource software development. NIST 800-53 control group SA ISO27001 A14
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?			x	
Change Control & Configuration Management *Quality Testing*	CCC-03	CCC-03.1	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards which focus on system availability, confidentiality, and integrity of systems and services.	Do you provide your tenants with documentation that describes your quality assurance process?	x			IBM Cloud IaaS customers are able to verify the accuracy of their deployed systems and services in real time via the customer portal. IBM Cloud IaaS controls related to Security and Availability can be assessed via review of the documentation provided by IBM Cloud IaaS's expert independent auditors in their certifications and reports.
		CCC-03.2		Is documentation describing known issues with certain products/services available?	x			IBM Cloud IaaS uses their notification system to give customers real time updates via email and the customer portal notification system.
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	x			The IBM Cloud IaaS system development life cycle process is all encompassing and includes every step from proposal, to approval, through development, review, testing, and finally approval/implementation. Risk assessment is also included in this process. IBM Cloud IaaS processes are validated frequently through internal audits and by independent auditors.
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	x			
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	x			IBM Cloud IaaS configure management controls restrict software installation to a limited small subset of employees and even then software installations must be approved. Most software installations are automated to eliminate the possibility of human error. ISO27001 A12.5.1
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	x			IBM Cloud IaaS's change management processes are validated frequently by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Cloud IaaS's SOC report provides an overview of the Change Management process. ISO27001 A.12
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	x			IBM Cloud IaaS gives the customer control when ordering a Virtual Machine to dictate where that Virtual Machine will reside, since IBM Cloud IaaS does not access, modify, delete, or retain data outside of the terms of the customer service agreement, the customer has control over what resources are being used.
		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	x			Dedicated hardware and virtual machines are assigned to customers pursuant to their specifications. This information is readily available within the customer portal and utilizes real time inventory asset tracking.
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?	x			Customers who wish to achieve geographic location can do so on the IBM Cloud IaaS system. To achieve geo location based authentication a customer could utilize SAML based Federation SSO, this would allow them to retain any authentication requirements they desire and then assert that to their IBM Cloud IaaS system.
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	x			IBM Cloud IaaS gives tenants control to select where their instances will reside during the ordering process, IBM Cloud IaaS encourages customers to spread their instances and store their data in multiple locations. IBM Cloud IaaS will not move customer data without first notifying the customer, unless required to by law.
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	x			
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data. The customer should follow a structured data-labeling standard that will help them achieve their desired level of compliance.
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	x			IBM Cloud IaaS gives tenants control to select where their instances will reside during the ordering process, IBM Cloud IaaS encourages customers to spread their instances and store their data in multiple locations. IBM Cloud IaaS will not move customer data without first notifying the customer, unless required to by law.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	x			IBM Cloud IaaS customers have control when ordering to dictate where the bare metal or virtual machine will reside. IBM Cloud IaaS does not touch data and will not move the customers data without first notifying the customer, unless required by law.
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud IaaS Customers wishing to ensure their data does not migrate beyond a defined geographic region can utilize bare metal servers with Intel TXT.
Data Security & Information Lifecycle Management *E-commerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	x			IBM Cloud IaaS allows and encourages customers to use their own encryption methods that meet their specific needs. IBM Cloud IaaS does offer NetApp AltaVault a cloud-integrate storage app that helps protect data using AES 256-bit encryption and transports data to the cloud using an SSLv3-TL Sv1 connection.

		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	x			IBM Cloud IaaS does not transmit replication data across the public network.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	x			IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud IaaS does not label media within the secured areas of the facilities to preserve the anonymity of the customers and tenants within. The customer should develop and maintain labeling and handling processes that will help them achieve their desired level of compliance. The customer should develop and maintain labeling and handling processes that will help them achieve their desired level of compliance. ISO27001 A8
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			x	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	x			IBM Cloud IaaS has secure development process and secure develeopment environments internally. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments. ISO27001 A14.2
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?	x			Responsibilities regarding data stewardship are documented and communicated in the IBM Cloud IaaS customer agreement. Please see the IBM Cloud IaaS customer agreement: http://static.softlayer.com/sites/default/files/assets/page/softlayer_msa.pdf
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	x			IBM Cloud IaaS employs a decommissioning and reclaim process for all hardware being reclaimed. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. ISO27001 A.8
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	x			The IBM Cloud IaaS sanitization procedure is public facing and available to customers upon request. The IBM Cloud IaaS customer service agreement documents the process for exiting the service arrangement.
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownershipby defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	x			IBM Cloud IaaS identified owners are designated for each of the processes and assets necessary for IBM Cloud IaaS operation as defined in ISO27001 standard. ISO27001 A8
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	x			IBM Cloud IaaS procurement and contract management maintain an inventory of all supplier relationships deemed critical.
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented?	x			IBM Cloud IaaS physical security parameters can include but are not limited to fences, walls, barriers, security guards, gates, electronic surveillance, video surveillance, physical authentication mechanisms, reception desks, and security patrols. NIST 800-53 PE ISO27001 A11
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	x			IBM Cloud IaaS security controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. NIST 800-53 IA
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another (e.g., offsite backups, business continuity failovers, replication)?	x			IBM Cloud IaaS allows tenants to select where their infrastructure will reside during the ordering process. IBM Cloud IaaS will not move customer data without first notifying the customer, unless required to by law.
Datacenter Security *Offsite Equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	x			IBM Cloud IaaS employs a decommissioning and reclaim process for all hardware being reclaimed or determined to be end of life. The reclaimed drive is wiped using the DOD 5220.22-M algorithms. If a device is determined to be end of life the hardware is wiped using the same method described above, then the device is physically crushed onsite. These measures are taken to protect customer's data. IBM Cloud IaaS's asset management and repurposing processes are validated frequently by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. Customers should leverage IBM Cloud IaaS's many third party certifications and assessments as evidence. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 CM ISO27001 A8
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	x			IBM Cloud IaaS engages third party auditors to validate our compliance with many different frameworks including but not limited to FedRAMP, ISO27001, SOC, PCI assessment, HIPAA. IBM Cloud IaaS customers should leverage certifications and assessments completed by third party auditors as evidence of security controls. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. NIST 800-53 PE ISO27001 standard A11
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	x			IBM Cloud IaaS maintains all core controls internally through frequent Key Control Objective testing and relies on third party auditors to validate our compliance with many different frameworks including but not limited to FedRAMP, ISO27001, SOC, PCI assessment, HIPAA. Customers should leverage IBM Cloud IaaS's many third party certifications and assessments. The IBM Cloud IaaS sanitization procedure is public facing and available to customers upon request. The IBM Cloud IaaS customer service agreement documents the process for exiting the service arrangement. IBM Cloud IaaS employees complete security awareness training which requires a strict pass rate percentage. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf.
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	x			IBM Cloud IaaS allows customers to select where their infrastructure will reside during the ordering process. IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement.
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	x			Physical security is controlled at many levels such as perimeter and building entrances, the physical security is not limited to, professional security staff, 24/7 video surveillance, security check point. Physical access points to the data halls all are recorded and monitored by onsite security, only authorized staff have the ability to access the data halls and they must authenticate a minimum of 2 times. Physical Security is reviewed by periodic internal audits as well as by third party audits such as FedRAMP, PCI, SOC, ISO27001
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	x			
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	x			Internally IBM Cloud IaaS key management controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. The customer should develop and maintain key management processes that will help them achieve their desired level of compliance.
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. Customers retain full control of their data, IBM Cloud IaaS allows them to use whatever encryption and key management controls they determine appropriate to meet their specific compliance initiatives. EKM-02 Internally IBM Cloud IaaS maintains cryptography keys in accordance to NIST 800-53 framework. IBM Cloud IaaS is audited on the controls put in place by third party auditors. NIST 800-53 control group SC12 ISO27001 A.10
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?			x	
		EKM-02.3		Do you maintain key management procedures?			x	
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?			x	
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?			x	
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud IaaS allows and encourages customers to develop and maintain encryption methods appropriate to help them achieve their desired level of compliance.
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?			x	
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?	x			
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	x			IBM Cloud IaaS process are reviewed by independent third party auditors for compliance with FedRAMP, SOC, PCI, ISO27001 NIST 800-53 control group SC
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?			x	IBM Cloud IaaS allows and encourages customers to use their own encryption methods they deem appropriate to meet their specific compliance initiatives.
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	x			IBM Cloud IaaS maintains keys management in accordance to NIST 800-53 framework. These controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Cloud IaaS process are reviewed internally during KCO audits ISO27001 A10
		EKM-04.3		Do you store encryption keys in the cloud?		x		
		EKM-04.4		Do you have separate key management and key usage duties?	x			
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system, and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	x			IBM Cloud IaaS maintains system baselines configurations for critical components. ISO27001 standard A.14, A.18
		GRM-01.2		Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	x			
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	x			Customers who have already developed server configurations to meet their specific business needs, can utilize IBM Cloud IaaS's Image Import and Export service allowing them to import their existing disk images into their IBM Cloud IaaS account. This is a free service to all IBM Cloud IaaS customers. More information here: http://knowledgelayer.softlayer.com/topic/image-templates
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	x			IBM Cloud IaaS provides third party audit reports, certifications, and responsibility matrixes to customers. These documents are comprised of information pertaining to IBM Cloud IaaS's core controls, processes, and procedures. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf.
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	x			IBM Cloud IaaS's Risk Assessment controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. IBM Cloud IaaS maintains controls that directly address the protection of personally identifiable information. IBM Cloud IaaS is certified ISO27018 compliant, establishing commonly accepted control objectives, controls, and guidelines for implementing measures to protect Personally Identifiable Information (PII). IBM Cloud IaaS's ISO27018 certificate can be found here: http://www.softlayer.com/sites/default/files/assets/page/softlayer-iso-27018.pdf
Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	x			Every IBM Cloud IaaS employee is presented with The Business Conduct Guidelines upon hire, and then refreshed and required to sign off on the BCGs every 6 months. Policy and Procedures are available to all internal personnel, updates are communicated to management to be incorporated in training and distributed via email to affected personnel.
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		x		IBM Cloud IaaS provides their ISO27001 certificate to customers but cannot release documentation on the IBM Cloud IaaS Information Security Management System as it is proprietary and confidential. IBM Cloud IaaS provides the ISO27001 certificate to tenants and perspective tenants. ISO27001 standard is a specification for an ISMS. The IBM Cloud IaaS Information Security Management System (ISMS), is maintained internally and validated via an external auditing group. IBM Cloud IaaS's ISO27001 certificate can be found here: http://www.softlayer.com/sites/default/files/assets/page/softlayer_iso27001_2016.pdf
		GRM-04.2		Do you review your Information Security Management Program (ISMP) at least once a year?	x			IBM Cloud IaaS reviews the ISMS at least annually, as required by ISO27001.
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	x			
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	x			IBM Cloud IaaS's information security and privacy policies align with ISO27001. IBM Cloud IaaS maintains all policies and processes internally and relies on third party auditors to validate compliance with different frameworks such as ISO27001. All third party requirements are implemented to align with ISO27001, these requirements are reviewed by external auditors to confirm compliance.
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?			x	
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?	x			
		GRM-06.4		Do you disclose which controls, standards, certifications, and/or regulations you comply with?	x			
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	x			IBM Cloud IaaS employees are presented with The Business Conduct Guidelines upon hire, and then refreshed and required to sign off on the BCGs every 6 months. IBM Cloud IaaS provides security training to employees to insure employees are educated on their responsibilities concerning information security. Violating IBM Cloud IaaS standards can result in internal investigation and disciplinary action.
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	x			
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	x			Updates to IBM Cloud IaaS policies, procedures, standards, and controls occur at least on an annual basis or as needed to meet diverse and developing compliance needs.
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	x			IBM Cloud IaaS does notify customers of privacy policy changes. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf.
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	x			IBM Cloud IaaS at minimum performs an annual review of all policies and procedures in accordance with ISO27001 standard. IBM Cloud IaaS is validated as being ISO27001 compliant by third party auditors.
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	x			IBM Cloud IaaS developed and maintains risk assessment processes aligned with the ISO27001 standard. Including risk assessments being performed at least annually. IBM Cloud IaaS is validated as being ISO27001 compliant by third party auditors.
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	x			IBM Cloud IaaS developed and maintains risk assessment processes aligned with the ISO27001 standard. IBM Cloud IaaS is validated as being ISO27001 compliant by third party auditors.
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Do you have a documented, organization-wide program in place to manage risk?	x			IBM Cloud IaaS risk management processes are aligned with ISO27001. IBM Cloud IaaS is validated as being ISO27001 compliant by third party auditors. The ISO27001 certificate can be found here http://www.softlayer.com/sites/default/files/assets/page/softlayer_iso27001_2016.pdf NIST 800-53 control group RA
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?	x			
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	x			Customers retain full control and responsibility to monitor their enviroment for privacy breaches. Customers can view IBM Cloud IaaS's SOC reports that provide details regarding controls in place to monitor the IBM Cloud IaaS environment
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	x			
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	x			IBM Cloud IaaS conducts background checks on all employees, as permitted in accordance with laws, regulations, and ethics. Customers can review the IBM Cloud IaaS's SOC reports that provide details regarding controls in place for background verification.
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	x			IBM Cloud IaaS requires all employees to complete training, a record of employee completion is maintained by IBM Cloud IaaS Trust and Assurance Team.
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	x			
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	x			All IBM Cloud IaaS personnel agree to Terms of Use and Rules of Behavior, including confidentiality agreements, upon first login to the IMS system then again every six months thereafter.
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	x			All IBM Cloud IaaS employees are required upon hire to complete SAT. Furthermore all employees are required to complete SAT training twice a year.
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	x			IBM Cloud IaaS requires all employees to complete training at least twice a year.
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	x			IBM Cloud IaaS termination and change of employment processes are in place and followed by Human Resources. These processes are maintained through internal audits and validated by independent auditors. ISO27001 A7.3.1
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	x			

Human Resources Portable / Mobile Devices	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	x			IBM Cloud IaaS does not touch the tenant's data. The customer should manage mobile security devices and access to their content to meet their specific compliance needs.	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	
Human Resources Non-Disclosure Agreements	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	x			IBM Cloud IaaS Legal and Trust and Assurance teams manages any changes to the Confidentiality Agreement.	S4.1.0	(S4.1.0) The entity's system availability, confidentiality, processing integrity and security performance is periodically reviewed and compared with the defined system availability and related security policies.	CC4.1	
Human Resources Roles / Responsibilities	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	x			The customer can find this type of information in the IBM Cloud IaaS Standard Customer service agreement.	S1.2.f	(S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security.		B.1
Human Resources Acceptable Use	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may access tenant data and metadata?	x			IBM Cloud IaaS employs the method of least privilege, allowing only the necessary access for users to accomplish their job function. IBM Cloud IaaS does not handle customer's data.	S1.2 S3.9	(S1.2) The entity's security policies include, but may not be limited to, the following matters: (S3.9) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC3.2 CC6.2	B.3
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (e.g., search engines, etc.)?	x			IBM Cloud IaaS Privacy Agreement contains information on data that is collected. http://www.softlayer.com/PRIVACY-AGREEMENT				
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?			x					
Human Resources Training / Awareness	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	x			All IBM Cloud IaaS employees complete Security Awareness Training twice a year. NIST 800-53 AT ISO27001 A7	S1.2.k S2.2.0	(S1.2.k) The entity's security policies include, but may not be limited to, the following matters: k. Providing for training and other resources to support its system security policies (S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users.	CC2.2 CC2.3	E.1
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	x			All IBM Cloud IaaS employees complete Security Awareness Training twice a year.				
Human Resources User Responsibility	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	x			IBM Cloud IaaS Policy and Procedures are always available to all internal personnel, updates are communicated to management to be incorporated in training and distributed via email to affected personnel. Every IBM Cloud IaaS employee is presented with The Business Conduct Guidelines upon hire, and then refreshed and required to sign off on the BCGs every 6 months.	S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality, processing integrity and security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	CC3.2	E.1
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	x							
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	x							
Human Resources Workspace	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?			x	IBM Cloud IaaS data management processes are in line with ISO27001 standard. ISO27001 A.7 and A.8	S3.3.0 S3.4.0	(S3.3.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	CC5.5 CC5.6	E.1
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	x							
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	x			IBM Cloud IaaS Security Operations Center creates rules around auditable events across the system. The system is scanned and these rules generate events in accordance with requirements. These auditable events are all logged and available for applicable teams to inspect or analyze. NIST 800-53 MP				
Identity & Access Management Audit Tools Access	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices.	S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1	
		IAM-01.2		Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	x			IBM Cloud IaaS logs and monitors all privileged access to the ISMS. These permissions are audited internally through frequent Key Control Objective testing and IBM Cloud IaaS relies on third party auditors to validate our permission compliance with many different frameworks including but not limited to FedRAMP, ISO27001, SOC, PCI assessment, HIPAA. NIST 800-53 AU				
Identity & Access Management User Access Policy	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices. IBM Cloud IaaS's SOC reports provide further details on user access. ISO27001 A.9	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		B.1
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		x		IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices. IBM Cloud IaaS's SOC reports provide further details on user access and removal of access. ISO27001 A.9				
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices. Access to privileged utilities is restricted to only personnel who require access and user activities are logged.	S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1	
Identity & Access Management Policies and Procedures	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	x			IBM Cloud IaaS's SOC reports provide further details on user access and removal of access. ISO27001 A.9				
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	x							
Identity & Access Management Segregation of Duties	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	x			Customers have the ability and responsibility to maintain segregation of duties with their service. Internally IBM Cloud IaaS restricts employees to the least access necessary to perform their job function, and segregates duties to prevent any one person from having full control. Customers should leverage the SOC2 report for this kind of information. ISO27001 A6.1.2	S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1	
Identity & Access Management Source Code Access Restriction	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	x			Logical Access to IBM Cloud IaaS systems is protected via authentication requirements and restricted to the least access necessary. Enforcement auditing is conducted by the IBM Cloud IaaS Security Operations Center. NIST 800-53 control group CM-5	S3.13.0	(S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.4	
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	x							
Identity & Access Management Third Party Access	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	x			IBM Cloud IaaS encourages customers to take advantage of IBM Cloud IaaS's extensive network of over 27 data centers around the globe to accomplish geographic resiliency. Customers can do this by purchasing instances in as many different locations as desired. IBM Cloud IaaS internally develops, maintains, updates, and disseminates Contingency Planning policies and procedures in line with ISO27001 requirements.	S3.1 x3.1.0	(S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system [availability, processing integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.	CC3.1	B.1 H.2
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	x			For the purpose of uptime and availability, IBM Cloud IaaS systems are designed with resiliency in mind. Customers have the ability to leverage IBM Cloud IaaS's systems and build their systems to have the level of resiliency. ISO27001 control group A9				
		IAM-07.3		Do you have more than one provider for each service you depend on?	x							
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	x			IBM Cloud IaaS operational redundancy and continuity is tested by IBM Cloud IaaS's independent expert auditors. The results of these tests are available within IBM Cloud IaaS's independent reports and certifications. Customers should leverage the SOC2 report for this information.				
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?			x	Customers can declare a disaster for their systems and take what steps they deem appropriate. IBM Cloud IaaS abuse and security can be contacted via email addresses located on the website.				
		IAM-07.6		Do you provide a tenant-triggered failover option?			x	IBM Cloud IaaS does access, modify, delete, or retain the customers data, customers have the ability to develop and maintain a failover option to meet their specific requirements.				
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?	x			IBM Cloud IaaS's business continuity processes are validated frequently by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA. For the safety of all customers infrastructure IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. Customers should leverage IBM Cloud IaaS's many third party certifications that test IBM Cloud IaaS Business Continuity and Disaster Recovery.				
Identity & Access Management User Access Restriction / Authorization	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	x			IBM Cloud IaaS customers control their data. Additionally customer instances are logically isolated from other customer instances via VLANs. Internally IBM Cloud IaaS has controls in place to limit access to systems via authentication requirements and restricted to the least access necessary. ISO27001 A.9	S3.2.0 S4.3.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls). (S4.3.0) Environmental, regulatory, and	CC3.3	
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?			x					
Identity & Access Management User Access Authorization	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	x			As part of IBM Cloud IaaS's onboarding process unique user identifiers and authenticators are only created and assigned, once HR has received management justification and approval.	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and authorization of new users. d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		
		IAM-09.2		Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	x			IBM Cloud IaaS maintains controls and trains employees on the threat of inappropriate insider access. IBM Cloud IaaS's external audits evaluate and validate the Logical Access Controls in place.				
Identity & Access Management User Access Reviews	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	x			IBM Cloud IaaS conducts user access review by internally auditing access rights and permissions during KCO audits, and validates these controls using multiple third party auditing firms to complete audits including but not limited to FedRAMP, SOC, ISO27001. More detail around IBM Cloud IaaS user access reviews can be found in the SOC reports. NIST 800-53 AC	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	x							
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	x							
Identity & Access Management User Access Revocation	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	x			Logical Access is automatically revoked when an employee is transferred or terminated. IBM Cloud IaaS's SOC reports provide more detail on user access revocation. ISO27001 A.9	S3.2.0	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: d. The process to make changes to user profiles. g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).		H.2
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	x							
Identity & Access Management User ID Credentials	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	x			IBM Cloud IaaS does not handle customers data, and leaves it up to the customer to decide what controls are necessary to meet the customers compliance requirements. IBM Cloud IaaS offers customers the ability to add and activate external authentication via the customer portal. More information here: http://knowledgelayer.softlayer.com/procedure/add-external-authentication-user	S3.2.b	(S3.2.b) b. Identification and authentication of users.	CC5.3	B.1 H.5
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	x							
		IAM-12.3		Do you support identity federation standards (e.g., SAML, SPML, W Federation, etc.) as a means of authenticating/authorizing users?	x							
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?		x						
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?			x					
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	x							
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?		x						
		IAM-12.8		Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	x			The customer should develop and maintain access management processes that will help them achieve their desired level of compliance. IBM Cloud IaaS SOC report details specific controls in place for IBM Cloud IaaS.				
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	x							
		IAM-12.10		Do you support the ability to force password changes upon first logon?	x							
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	x							
Identity & Access Management Utility Programs Access	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices. Access to privileged utilities is restricted to only personnel who require access and user activities are logged. IBM Cloud IaaS's SOC reports provide further details on user access and removal of access.	S3.2.g	(S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).	CC5.1	
		IAM-13.2		Do you have the capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	x							
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	x							
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	x			IBM Cloud IaaS processes around Audit Logging and Intrusion detection are developed based on the NIST 800-53. Audit logs are stored and retained to FISMA standards. These logs are protected by active directory user credentials and physical access controls with all access and actions logged and monitored.	S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	CC6.2	G.7 G.8 G.9 J.1 L.2
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	x							
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	x							
		IVS-01.4		Are audit logs centrally stored and retained?	x							
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	x							
Infrastructure & Virtualization Security Change Detection	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?		x		Once a customer takes control of their virtual machine they are able to control what resources are being used.				
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?		x						
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	x			IBM Cloud IaaS clocks are synchronized to NIST time servers via NTP.	S3.7	(S3.7) Procedures exist to identify, report, and act upon system security breaches and other incidents.	CC6.2	G.7 G.8
Infrastructure & Virtualization Security Capacity / Resource Planning	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			x	IBM Cloud IaaS maintains capacity and resource planning in alignment with ISO27001 and these efforts are validated by external auditors to confirm IBM Cloud IaaS is ISO27001 compliant. ISO27001 A12.1.3	A3.2.0 A4.1.0	(A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. (A4.1.0) The entity's system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.	A1.1 A1.2 CC4.1	
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	x							
		IVS-04.3		Do your system capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	x							
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	x							
Infrastructure & Virtualization Security Management - Vulnerability Management	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?	x			IBM Cloud IaaS offers basic vulnerability scans to customers via the customer portal. These scans, as well as the scans used by the IBM Cloud IaaS Security Operations center to secure IBM Cloud IaaS's own information systems supporting the services are virtualization aware.				
Infrastructure & Virtualization Security Network Security	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	x			The IBM Cloud IaaS website offers the latest industry-leading security solutions to help customer create a comprehensive security strategy. The customer has the ability to Create a Multi-Layer security Strategy as fits their compliance needs. More information here: http://www.softlayer.com/SECURITY IBM Cloud IaaS customers should also leverage the SOC2 report and ISO27001 certificate as a foundation to build their compliance controls.	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	G.2 G.4 G.15 G.16 G.17 G.18 I.3
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	x			IBM Cloud IaaS's network security controls are built on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. IBM Cloud IaaS implements logical boundaries, vulnerability scans, and monitoring of the Network. More information here: http://www.softlayer.com/our-platform%20				
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	x			IBM Cloud IaaS Network Security Management is regularly reviewed as part of internal KCO audits and validated by multiple third party auditing firms that conduct audits including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment. IBM Cloud IaaS implements job duty segmentation and an automated permissions system to limit access to job specific functions throughout the system				
		IVS-06.4		Are all firewall access control lists documented with business justification?	x							
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?			x	IBM Cloud IaaS does no operating system hardening for customer, this is something the customer has the ability to do as they see fit with their compliance needs.				
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement, customers have the ability and responsibility to implement separate environments for production and test processes. Customers should develop production and non-production environments in compliance with their defined compliance goals in mind.	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	B.1
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	x			IBM Cloud IaaS IaaS customers can leverage IBM Development and Test Environment for guidance on how to create suitable production and test environments.				
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	x			IBM Cloud IaaS network segmentation is implemented internally in line with the ISO27001 standard. IBM Cloud IaaS is validated by an external auditor to be in adherence to the ISO27001 standard. ISO27001 A.12.1.4 ISO27001 A.14.2				
Infrastructure & Virtualization Security Segmentation	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	x			IBM Cloud IaaS customers have the ability and responsibility to implement network segmentation in compliance with their defined compliance goals. IBM Cloud IaaS offers hardware and software firewall options that customers should consider when implementing their security strategy. More information here: http://www.softlayer.com/FIREWALLS Internally IBM Cloud IaaS firewall uses 3 interfaces to protect and maintain compliance with ongoing compliance efforts. IBM Cloud IaaS segmentation is implemented in line with the ISO27001 standard, these controls are validated by an external auditor.	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	G.17
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory, and contractual requirements?	x							
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	x							
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	x							
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. But strongly encourages all customers to use encryption mechanisms for data at rest and in transit to meet their specific requirements.				
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	x			IBM Cloud IaaS provides customers the ability, however it is customers resonsibility to maintain proper network segregation to create and maintain production and non-production environments. The IBM Cloud IaaS private network is available for all customers.				
Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	x			IBM Cloud IaaS identifies and maintains all requirements for access within the Logical Access Management Policy which is based on least privilege and best practices. Access to privileged utilities is restricted to only personnel who require access and user activities are logged.				

Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	x			IBM Cloud IaaS has extensive policies and processes in place to protect the IBM Cloud IaaS network. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. These policies and procedures are reviewed by external auditors conducting assessments including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI.
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	x			
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	x			
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	x			IBM Cloud IaaS provides customers the ability, however it is customer's responsibility to maintain proper network segregation to align with their compliance needs. Internally IBM Cloud IaaS network architecture is validated against the ISO27001 standard.
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	x			IBM Cloud IaaS implements technical measures when maintaining our Infrastructure & Virtualization Security controls to detect and insure timely response to attacks on the IBM Cloud IaaS system. These controls are maintained through frequent internal audits and are validated by external auditors through assessments including but not limited to FedRAMP, ISO27001, SOC, PCI, and HIPAA.
Interoperability & Portability *APIs*	IPY-01	IPY-01.1	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	x			The IBM Cloud IaaS API has more than 3,000 documented methods across 180 discrete services. All customers have full, free access to the entire automated portfolio of services. More information on the IBM Cloud IaaS API can be found here: http://www.softlayer.com/API
Interoperability & Portability *Data Request*	IPY-02	IPY-02.1	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	x			
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?			x	IBM Cloud IaaS customers are responsible for their data and have the ability to decide the method used to migrate applications to and from their IBM Cloud IaaS infrastructure.
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?			x	IBM Cloud IaaS has extensive policies and processes in place to protect the IBM Cloud IaaS network. IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf. These policies and procedures are reviewed by external auditors conducting assessments including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI.
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	x			IBM Cloud IaaS customers are responsible for their data and have the ability to decide the method used to migrate applications and data to and from their IBM Cloud IaaS infrastructure. Information on storage options offered by IBM Cloud IaaS can be found here: http://www.softlayer.com/cloud-storage
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?			x	
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	x			The IBM Cloud IaaS Security Operations Center routinely scans internal and external facing non-customer apps for vulnerabilities. The Security Operations Center reports discovered vulnerabilities to the appropriate system owners for remediation in accordance with all applicable standards. IBM Cloud IaaS engages third party groups as well as IBM to conduct penetration testing as prescribed by industry best practices. IBM Cloud IaaS hypervisors are included and reguarly validated by third party auditors conducting assessments including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI.
		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		x		IBM Cloud IaaS does not have solution specific hooks, the IBM Cloud IaaS Security Operations Center scans and monitors vulnerabilities 24/7.
Mobile Security *Anti-Malware*	MOS-01	MOS-01.1	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. IBM Cloud IaaS utilized anti-malware as well as continuous monitoring to insure compliance with ISO27001 standard. ISO27001 standard control A.12.2
Mobile Security *Application Stores*	MOS-02	MOS-02.1	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
Mobile Security *Approved Applications*	MOS-03	MOS-03.1	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			x	
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04.1	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			x	
Mobile Security *Awareness and Training*	MOS-05	MOS-05.1	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			x	
Mobile Security *Cloud Based Services*	MOS-06	MOS-06.1	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			x	
Mobile Security *Compatibility*	MOS-07	MOS-07.1	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
Mobile Security *Device Eligibility*	MOS-08	MOS-08.1	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			x	
Mobile Security *Device Inventory*	MOS-09	MOS-09.1	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			x	
Mobile Security *Device Management*	MOS-10	MOS-10.1	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			x	
Mobile Security *Encryption*	MOS-11	MOS-11.1	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			x	
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and is enforced through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			x	
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case that a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			x	
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			x	
Mobile Security *Lockout Screen*	MOS-14	MOS-14.1	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
Mobile Security *Operating Systems*	MOS-15	MOS-15.1	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			x	
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			x	
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			x	
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			x	
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			x	
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			x	
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			x	
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			x	
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			x	No mobile devices directly access the IBM Cloud IaaS cloud service management networks or delivery networks. Customers have the ability and responsibility to manage mobile security devices and access as they deem appropriate to meet their specific compliance initiatives.
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			x	
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			x	
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			x	
Security Incident Management, E-Discovery, & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	x			IBM Cloud IaaS maintains points of contract with local authorities in accordance with contracts, regulations, and IBM Cloud IaaS's many compliance requirements including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment. ISO27001 A6
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	x			IBM Cloud IaaS's incident response plan was developed on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. IBM Cloud IaaS Trust and Assurance maintains all core controls through internal KCO audits and validates these controls using multiple third party auditing firms to conduct audits including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment.
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		x		IBM Cloud IaaS internally maintains an incident response policy and plan both developed to ensure that IBM Cloud IaaS delivers world class, secure, on-demand virtual data center services. The incident response plan details purpose, roles and responsibilities, preparation, detection and analysis, containment, recovery, post-incident activity and has been developed in alignment with the NIST 800-53 standards and ISO27001 standards. Below is an overview of the 5 phased approach IBM Cloud IaaS has implemented: 1. Preparation Phase - Information Security Policies and Procedures are maintained and available to all security operations personnel. - Vulnerability Management is a function of the Security Operations Center, vulnerability scans are conducted and vulnerability intelligence is collected internally as well as from outside sources. - Continuous Monitoring by the Security Operations Center - Control Auditing - Incident Response Team Structure, in the event of an incident a response team will be formed consisting of at least one incident response lead and one technical lead. - Testing of Incident Response Plan is conducted internally as well as tested by external auditors on a regular basis. 2. Detection and Analysis Phase: - Methods of detection, there are many methods of detections. There methods are monitored on a 24 hour basis. - Event Analysis will begin when an incident is suspected, should an incident be confirmed, a full investigation will begin. - Notification will be sent to the Security Incident distribution list. - Response - Event Logging, all events are to be logged and are to include facts and concrete findings - Evidence Collection will be implemented being mindful of requirements for uptime and authentication, and also for containment and eradication. - Exit Criteria 3. Containment Phase: - Key Decisions, a list of key decisions is laid out for consideration. - Incident Characterization, to best determine the course of action the type of incident must first be determined. - Notifications, depending on the severity and scope of the incident there are internal and external notifications that may be required. - Incident Containment - Incident Isolation - Root Cause Analysis and Identification - Determine rootkit potential - Recommend and implement additional controls - Evaluate risk tolerance and remediate vulnerabilities 4. Recovery Phase - Contingency Operations - Implement additional monitoring 5. Post-Incident Activity Phase - Post-Incident Report - Closure of incident happens only after the incident report has been submitted to the appropriate personnel - After Action includes in depth discussions to identify and recommend improvements based on lessons learned.
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	x			
		SEF-02.4		Have you tested your security incident response plans in the last year?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	x			
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	x			
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	x			
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	x			
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	x			
Security Incident Management, E-Discovery, & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	x			
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?		x		IBM Cloud IaaS's incident response plan was developed on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. IBM Cloud IaaS Trust and Assurance maintains all core controls through internal KCO audits and validates these controls using multiple third party auditing firms to conduct audits including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment. The IBM Cloud IaaS ISO27001 certificate can be found here: http://www.softlayer.com/sites/default/files/assets/page/softlayer_iso27001_2016.pdf
Supply Chain Management, Transparency, and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?			x	IBM Cloud IaaS does not access, modify, delete, or retain customer data outside the terms of the customer service agreement. The customer should develop and maintain processes to insure data quality and integrity that will help them achieve their desired level of compliance. IBM Cloud IaaS data quality and integrity is assessed and validated using multiple third party auditing firms to conduct audits including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment.
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	x			
Supply Chain Management, Transparency, and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	x			IBM Cloud IaaS's incident response process including reporting was developed on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. IBM Cloud IaaS Trust and Assurance maintains all core controls through internal KCO audits and validates these controls using multiple third party auditing firms to conduct audits including but not limited to FedRAMP, SOC, ISO27001, ISO27017, ISO27018, PCI assessment.
Supply Chain Management, Transparency, and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	x			IBM Cloud IaaS manages capacity as defined in the ISO27001 standard. IBM Cloud IaaS's capacity management controls are maintained by the Trust and Assurance team and validated by multiple third party auditing firms who conduct assessments. NIST 800-53 CP
		STA-03.2		Do you provide tenants with capacity planning and use reports?	x			
Supply Chain Management, Transparency, and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	x			IBM Cloud IaaS's core controls are built on the foundation of NIST 800-53 with special consideration of other relevant standards such as ISO27001. IBM Cloud IaaS Trust and Assurance maintains all core controls through internal KCO audits. Policy and Procedure review and assessment of conformance is part of these internal audits conducted.
Supply Chain Management, Transparency, and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	x			IBM Cloud IaaS manages its own infrastructure, to compensate for the need to control suppliers, also IBM Cloud IaaS does not outsource any development. For other agreements IBM Cloud IaaS legal as well as procurement team monitors selected outsourced providers to insure compliance with laws. Any personnel working on or directly able to affect the IBM Cloud IaaS system are treated as IBM Cloud IaaS employees and must complete the same screening process, including but not limited to, background checks, NDA acknowledgement, and Business Conduct Guidelines acknowledgement.
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	x			
		STA-05.3		Does legal counsel review all third-party agreements?	x			IBM Cloud IaaS Legal counsel is required to review all third-party agreements. All third party agreements include provisions to protect IBM Cloud IaaS information and assets, including but not limited to, separate non-disclosure agreements, or confidentiality provisions in the contract.
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	x			
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?			x	No-sub processors are utilized in support of IBM Cloud IaaS services.
Supply Chain Management, Transparency, and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	x			IBM Cloud IaaS has agreements with key third party suppliers with defined expectations and implements relationship management tools where applicable with third-party suppliers. These management mechanisms include frequent validation that the supplier is meeting the expectations as defined in agreements. IBM Cloud IaaS supplier management processes are validated by external auditors as part of compliance with SOC and ISO27001.
Supply Chain Management, Transparency, and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	x			
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	x			
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	x			
		STA-07.4		Do you review all agreements, policies, and processes at least annually?	x			Updates to IBM Cloud IaaS policies, procedures, standards, and controls occur at least on an annual basis or as needed to meet diverse and developing compliance needs. IBM Cloud IaaS agreements are reviewed at time of renewal.
Supply Chain Management, Transparency, and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	x			IBM Cloud IaaS security documentation, including but not limited to policies and procedures, is proprietary and confidential; IBM Cloud IaaS cannot provide these documents to customers or to entities acting on their behalf.
		STA-08.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	x			
Supply Chain Management, Transparency, and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?	x			Customers can perform scans of their systems as long as they do not affect other IBM Cloud IaaS customers. IBM Cloud IaaS encourages customers to inform the Security Operations Center prior to penetration test to insure they are not shut down, if a customer's scans begin affecting other customers they will be blocked.
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	x			The IBM Cloud IaaS Security Operations Center routinely scans internal and external facing non-customer apps for vulnerabilities. The Security Operations Center reports discovered vulnerabilities to the appropriate system owners for remediation in accordance with all applicable standards. IBM Cloud IaaS engages third party groups as well as IBM to conduct penetration testing as prescribed by industry best practices.
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	x			IBM Cloud IaaS has anti-malware in place in compliance with ISO27001 standard. IBM Cloud IaaS processes around anti-malware and malicious software are in compliance with ISO27001 standard and tested internally and by external auditors. ISO27001 standard control group A.12.2
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	x			
Threat and Vulnerability	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	x			The IBM Cloud IaaS Security Operations Center routinely scans internal and external facing non-customer apps for vulnerabilities. The Security Operations Center reports

Management Vulnerability / Patch Management		TVM-02.2	detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	x			discovered vulnerabilities to the appropriate system owners for remediation in accordance with applicable standards.		infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.					Subsec. 4.7.3			COBIT 4.1 DS5.9	APO13.02 BAI06.01 BAI06.02 BAI06.03 BAI06.04 DSS01.01 DSS01.02 DSS01.03 DSS03.05 DSS05.01 DSS05.03 DSS05.07		Management > Vulnerability Management				6.03.05. (c) 6.07.01. (o)		NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 RA-5 (1) NIST SP 800-53 R3 RA-5 (2) NIST SP 800-53 R3 RA-5 (3) NIST SP 800-53 R3 RA-5 (6) NIST SP 800-53 R3 RA-5 (9) NIST SP 800-53 R3 SC-30 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-5			45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)		A.12.6.1	8.1*partial, A.14.2.3 A.12.6.1				4.2 CIP-005-3a - R1 - R1.1 CIP-007-3 - R3 - R3.1 - R8.4	CP-10 RA-5 SA-7 SI-1 SI-2 SI-5			12.4.4.C.02. 12.4.4.C.03. 12.4.4.C.04. 12.4.4.C.05. 12.4.4.C.06. 12.4.5.C.01. 12.4.6.C.01. 12.4.7.C.01. 14.1.6.C.01. 14.1.7.C.01. 14.1.7.C.02. 14.1.8.C.01. 14.1.8.C.02. 14.1.9.C.01. 14.1.10.C.01. 14.1.10.C.02. 14.1.10.C.03. 14.1.11.C.01. 14.1.11.C.02. 14.1.11.C.03. 14.1.12.C.01.		PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1	6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3		6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3	1.4 1.5
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	x																																											PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0				
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?		x		IBM Cloud IaaS vulnerabiltiy and patch management procedures and processes are part of the core controls that are maintained internally and validated by external auditors. IBM Cloud IaaS cannot release the results of these scans, as it would put systems and customers at risk. Customers should leverage the SOC report and ISO27001 certificate as these controls are tested within both of these assessments by third party auditors. Customers are permitted to scan their environment at any time.																																								PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0				
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?	x			IBM Cloud IaaS's patching procedures allows rapid patching across systems.																																								PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0				
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?		x		IBM Cloud IaaS provides patched images of any provisioned software. Subsequent patching processes are up to the individual customer. Patching procedures for IBM Cloud IaaS systems supporting the services are tested as part of the internal and external audit process. The independent third party audit results are available to customers to review IBM Cloud IaaS's implementation.																																								PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X				
Threat and Vulnerability Management Mobile Code	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	x			IBM Cloud IaaS customers are responsible for thee installation and use of mobile code on their systems to fit their own requirements.	S3.4.0 S3.10.0	(S3.4.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC5.6 CC7.1		G.20.12, I.2.5			SA-15			APO01.03 APO13.01 APO13.02 DSS05.01 DSS05.02 DSS05.03 DSS05.04	312.8 and 312.10	SRM > Infrastructure Protection Services > End Point - White Listing	shared	x	Domain 10	6.03. (g)	Article 17						09.k	A.10.4.2 A.12.2.2	A.12.2.1		Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11			SC-18		3 3.1 3.2 3.3 3.4 3.5							6.9
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	x																																															
© Copyright 2014 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire CAIQ Version 3.0.1" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire v3.0.1 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v3.0.1 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v3.0.1 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Consensus Assessments Initiative Questionnaire 3.0.1 (2014). If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.																																																

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ) V3.0.1 GUIDING DOCUMENT

INTENT OF THIS TAB: To assist reviewers/users of document to understand both the intent and

GUIDING PRINCIPLES:

- Questionnaire is organized using CSA 16 governing & operating domains divided into "control areas" within CSA's Controls Matrix structure

- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile

- CAIQ is not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area

- Each question should be able to be answered yes or no

- If a question can't be answered yes or no then it was separated into two or more questions to allow yes or no answers.

- Questions are intended to foster further detailed questions to provider by client specific to client's cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all follow-on

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes	CCM v3.0.1 Compliance Mapping
					Yes	No	Not Applicable		AICPA TSC 2009
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	Yes			MOBI leverages frameworks from both ISO27001 and NIST for ensuring system, software, and network security.	S3.10.0
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes			Tests are performed each month, with PCI Compliance certification every quarter. Our compliance vendor performs both vulnerability and penetration test assessments for us. We have provided the IPs to our compliance vendor so that tests are performed on key systems of our infrastructure. Unfortunately, MOBI cannot share the results with any customer. Our SaaS platform is multi-tenant, so no specific instance will be instantiated for customers.	
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	Yes				
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	Yes				
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes				
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	Yes				S3.2a
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	Yes				
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	Yes				S3.4
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	Yes			MOBI has designed its data security architecture around NIST STIG guidelines outlined by FedRAMP.	
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		No			S4.1.0 S4.2.0
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	Yes				S4.1.0 S4.2.0
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes				
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes				
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes				
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes				
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	Yes				
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	Yes				
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?		No			
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes			Data is segmented logically. We have very specific domain logic built into our application to ensure that only a specific customer's data is accessed or displayed when a cutomer user accesses our system.	
		AAC-03.2		Do you have capability to recover data for a specific customer in the case of a failure or data loss?	Yes				
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?		No			
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes				
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide tenants with geographically resilient hosting options?		No		Geographic redundancy is on our road map but with no current ETA.	A3.1.0 A3.3.0 A3.4.0
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?		No		MOBI has designed its infrastructure to be fault-tolerant and to have fail-over resources immediately available. MOBI has a replicated environment at a different geographic facility.	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes				A3.3
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	Yes			The MOBI Infrastructure Overview (v1.5) documentation provides for a network diagram and high-level view of data flows.	A3.2.0 A3.4.0
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?		No			
Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Yes				S3.11.0 A.2.1.0
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	Yes				A3.1.0 A3.2.0
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		No			A3.1.0 A3.2.0
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	Yes				A3.2.0 A4.1.0
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?		No		Access to MOBI's cloud infrastructure is not directly unavailable to customer.	
		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		No		MOBI is a managed, cloud-based, SaaS offering only.	
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		No		MOBI is a managed, cloud-based, SaaS offering only.	
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	Yes				
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes				A3.2.0
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	Yes			MOBI can generate reports on demand, with a limit of 1 request per month.	A3.1.0 A3.3.0 A3.4.0
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	Yes			All aspects of infrastructure security and performance are monitored.	

		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	Yes																																						
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes				S2.3.0	(S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.	CC3.2		G.1.1	45 (B)		OP-01	COBIT 4.1 DS13.1	APO01 APO07.01 APO07.03 APO09.03 DSS01.01		SRM > Policies and Standards > Operational Security Baselines	shared	x	Domain 7, 8	6.03. (c)		NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-4 (1) NIST SP 800-53 R3 MA-4 (2) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1) NIST SP 800-53 R3 SA-12		8.2.1		Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1	Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1		Commandment #1 Commandment #2 Commandment #3 Commandment #6 Commandment #7			CM-2 CM-3 CM-4 CM-5 CM-6 CM-9 MA-4 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-12					PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	4.3, 10.8, 11.1.2, 12.1 12.2 12.3 12.4 12.5, 12.5.3, 12.6, 12.6.2, 12.10
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?	Yes				A3.3.0 A3.4.0 I3.20.0 I3.21.0	(A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies. (A3.4.0) Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies. (I3.20.0) Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies. (I3.21.0) Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.	A1.2 A1.3 I3.21		D.2.2.9	36 (B)	Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.5.2	DG-04	COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	BAI09.01 BAI09.02 BAI09.03 DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.07 MEA03.01	312.3	BOSS > Data Governance > Data Retention Rules	shared	x	Domain 5	6.03. (h) 6.07.01. (c)	Article 6(1) e	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-2 (1) NIST SP 800-53 R3 CP-2 (2) NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3) NIST SP 800-53 R3 CP-7 (5) NIST SP 800-53 R3 CP-8 NIST SP 800-53 R3 CP-8 (1) NIST SP 800-53 R3 CP-8 (2) NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-9 (1) NIST SP 800-53 R3 CP-9 (3)		5.1.0 5.1.1 5.2.2 8.2.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) (New) 45 CFR 164.316(b)(2)(i) (New)	Clause 4.3.3 A.10.5.1 A.10.7.3	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1 A.8.2.3	EAR 15 § 762.6 Period of Retention EAR 15 CFR § 786.2 Recordkeeping	Commandment #11	Chapter II Article 11, 13	CIP-003-3 - R4.1	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11	FTC Fair Information Principles Integrity/Security Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/reports/privacy3/fairinfo.shtm	6.4 13.1	PA10 PA29	BSGP SGP	PCI DSS v2.0 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0 9.9.1 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 10.7	3.1 3.1.a 3.2 9.9.1 9.5, 9.5.1 9.6, 9.7, 9.8 10.7, 12.10.1
		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?		No		MOBI's policy is to cooperate with all government law agencies that present a valid warrant to collect data.																																			
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes																																						
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	Yes			MOBI's current RPO is 24 hours for a database backup and the most recent production-certified configuration file. RTO is 1.25 hours for any server that experiences a disaster and must be rebuilt. MOBI has built a fault-tolerant infrastructure to withstand minor failures so that in the event of a disaster we can still serve our customers.																																			
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Yes			CODE REVIEW MOBI maintains an authoritative code style guide and utilizes linters to flag code changes that do not conform to defined standards. This practice ensures quality, consistency, and clarity of code contributions. MOBI developers are required to write test coverage for all code implementations. All code submitted for pull request will automatically run the entire test suite to ensure integrity of the change and mitigate implications to other areas of the application.	S3.12.0 S3.10.0 S3.13.0	(S3.12.0) Procedures exist to maintain system components, including configurations consistent with the defined system security policies. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.2 CC7.1 CC7.4	I.2	I.1.1, I.1.2, I.2. 7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-01	COBIT 4.1 A12, A 16.1	APO01.02 APO01.06 BAI02.04 BAI06.01		ITOS > IT Operation > Architecture Governance	shared	x	None	6.03. (a)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7)		1.2.6		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7 A.18.1.3 A.18.1.4		Commandment #1 Commandment #2 Commandment #3			CA-1 CM-1 CM-9 PL-1 PL-2 SA-1 SA-3 SA-4		12.1			PCI DSS v2.0 6.3.2	6.3.2, 12.3.4
		CCC-01.2		Is documentation available that describes the installation, configuration and use of products/services/features?		No		MOBI is a managed, cloud-based, SaaS offering only.																																			
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	Yes				S3.10.0 S3.13	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.1 CC7.4	C.2 I.1 I.2 I.4	C.2.4, G.4, G6, I.1, I.4.4, I.4.5, I.2.7.2, I.2.8, I.2.9, I.2.15, I.2.18, I.2.22.6, I.2.7.1, I.2.13, I.2.14, I.2.17, I.2.20, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14, I.3, J.1.2.10, L.7, L.9, L.10	27 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-04		APO07.06 APO09.03 APO09.04 APO10.01 APO10.04 APO10.05 APO11.01 APO11.02 APO11.04 APO11.05		ITOS > IT Operation > Architecture Governance	shared	x	None			NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1) NIST SP 800-53 R3 SA-12				A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.5 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3 8.1* (partial) A.14.2.4 8.1* (partial) A.14.2.7 A.12.6.1 A.16.13 A.18.2.2 A.18.2.3		Commandment #1 Commandment #2 Commandment #3			SA-4 SA-5 SA-8 SA-9 SA-10 SA-11 SA-12 SA-13		2.2 4.1	PA17	SGP	PCI DSS v2.0 3.6.7 PCI DSS v2.0 6.4.5.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 8.5.1 PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.2b PCI DSS v2.0 9.3.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 11.5 PCI DSS v2.0 12.3.1 PCI DSS v2.0 12.3.3	2.1, 2.2.4, 2.3, 2.5 3.3, 3.4, 3.6 4.1, 4.2 6.3.1, 6.3.2, 6.4.2, 6.4.3, 6.4.4, 6.4.5.2 6.7 7.1, 7.1.3, 7.1.4 8.3, 8.5.1, 8.7 9.1 9.1.2 9.2 10.5 11.5 12.3 12.8
		CCC-02.2		Do you have controls in place to detect source code security defects for any outsourced software development activities?	Yes																																						
Change Control & Configuration Management *Quality Testing*	CCC-03	CCC-03.1	Organization shall follow a defined qualty change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	Do you provide your tenants with documentation that describes your quality assurance process?	Yes			The MOBI Code Review Process for details on MOBI's quality assurance policy.	A3.13.0 C3.16.0 I3.14.0 S3.10.0 S3.13	(A3.13.0, C3.16.0, I3.14.0, S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability, confidentiality of data, processing integrity, systems security and related security policies. (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.1 CC7.1 CC7.1 CC7.1 CC7.4		C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7, I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I.2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-03	COBIT 4.1 PO 8.1	APO11.01 APO11.02 APO11.04 APO11.05 BAI02.04 BAI03.06 BAI03.08 BAI07.03 BAI07.05		ITOS > Service Support > Release Management	shared	x	None	6.03.01. (b) 6.03.01. (d)		NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-4 (1) NIST SP 800-53 R3 SA-4 (4) NIST SP 800-53 R3 SA-4 (7) NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-5 (1) NIST SP 800-53 R3 SA-5 (3) NIST SP 800-53 R3 SA-8 NIST SP 800-53 R3 SA-10 NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)		9.1.0 9.1.1 9.2.1 9.2.2		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	A.6.1.1 A.12.1.1 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* partial A.14.2.2 8.1* partial A.14.2.3 8.1* partial A.14.2.4 A.12.6.1 A.16.1.3 A.18.2.2 A.18.2.3		Commandment #1 Commandment #2 Commandment #3			CM-1 CM-2 SA-3 SA-4 SA-5 SA-8 SA-10 SA-11 SA-13		12.1 14.1 14.2			PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.4	6.1 6.2 6.3 6.4 6.5 6.6 6.7
		CCC-03.2		Is documentation describing known issues with certain products/services available?	Yes			A document can be produced and shared that identifies all packages that have been updated due to a CVE. Updates are installed on a monthly basis, with security updates being installed within 15 days of release (depending on severity). This ensures that our systems are always patched and secured with the latest code.																																			
		CCC-03.3		Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	Yes																																						
		CCC-03.4		Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	Yes																																						
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes			Yes. Only MOBI's Systems Administrators have access to an account that can elevate to an administrative user to install software. All requests are processed through the IT Ticket system, if a new software install is required by our Development Teams. In addition to logical controls, MOBI also employs the use of SELinux to prevent any process from running operations outside its domain (i.e. installing software).	A3.6.0 S3.5.0 S3.13.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (S3.5.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC5.5 CC5.8 CC7.4	G.1 I.2	G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-05		APO13.01 BAI06.01 BAI10 DSS05.03 DSS05.04 DSS05.05 DSS05.07 DSS06.03	312.8 and 312.10	ITOS > Service Support > Configuration Management -> Software Mangement	shared	x	None			NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-7 (1) NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 CM-8 (1) NIST SP 800-53 R3 CM-8 (3) NIST SP 800-53 R3 CM-8 (5) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-3 (1) NIST SP 800-53 R3 SI-3 (2) NIST SP 800-53 R3 SI-3 (3) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6)		3.2.4 8.2.2		A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3	A.6.1.2 A.12.2.1 A.9.4.4 A.9.4.1 A.12.5.1 8.1* (partial) A.14.2.4		Commandment #1 Commandment #2 Commandment #3 Commandment #5 Commandment #11			CM-1 CM-2 CM-3 CM-5 CM-7 CM-8 CM-9 SA-6 SA-7 SI-1 SI-3 SI-4 SI-7	FTC Fair Information Principles Involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers . - http://www.ftc.gov/reports/privacy3/fairinfo.sht	14.1				1.3.3 2.1, 2.2.2 3.6 4.1 5.1, 5.2, 5.3, 5.4 6.2 7.1 9.1 9.1.1 9.1.2 9.1.3 9.2 9.3 9.4 9.4.1 9.4.2 9.4.3 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7 11.1, 11.4, 11.5 12.3
Change Control & Configuration Management *Production Changes*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA).	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		No		MOBI will answer any specific questions required, but does not supply documentation to customers about specific internal practices. These practices are subject to SOC audit.	A3.16.0 S3.13.0	(A3.16.0, S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	CC7.4 CC7.4		I.2.17, I.2.20, I.2.22		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	RM-02	COBIT 4.1 A16.1, A17.6	BAI06.01 BAI06.02 BAI06.03 BAI06.04 BAI07.01 BAI07.03 BAI07.04 BAI07.05 BAI07.06		ITOS > Service Support > Release Management	shared	x	None	6.03. (a)		NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CA-7 (2) NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-2 (1) NIST SP 800-53 R3 CM-2 (3) NIST SP 800-53 R3 CM-2 (5) NIST SP 800-53 R3 CM-3 NIST SP 800-53 R3 CM-3 (2) NIST SP 800-53 R3 CM-5 NIST SP 800-53 R3 CM-5 (1) NIST SP 800-53 R3 CM-5 (5) NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 CM-6 (1) NIST SP 800-53 R3 CM-6 (3) NIST SP 800-53 R3 CM-9 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-2 (2) NIST SP 800-53 R3 SI-6 NIST SP 800-53 R3 SI-7 NIST SP 800-53 R3 SI-7 (1)		1.2.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3		Commandment #1 Commandment #2 Commandment #3 Commandment #11		CIP-003-3 - R6	CA-1 CA-6 CA-7 CM-2 CM-3 CM-5 CM-6 CM-9 PL-2 PL-5 SI-2 SI-6 SI-7	AR- 4. Privacy Monitoring and Auditing. Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) coordinates monitoring and auditing efforts with information security officials and	12.1 12.4	PA14	SGP	PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.3.2 PCI DSS v2.0 6.4 PCI DSS v2.0 6.1	1.1.1 6.3.2 6.4.5
Data Security & Information Lifecycle Management *Classification*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?		No			S3.8.0 C3.14.0	(S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.	CC3.1 CC3.1		D.1.3, D.2.2			DG-02	COBIT 4.1 PO 2.3, DS 11.6	APO01.06 APO03.02 APO08.01 APO09.03 APO13.01 BAI09.01 BAI09.02 BAI09.03 DSS04.07 DSS05.04 DSS05.05 DSS06.06	312.3	BOSS > Data Governance > Data Classification	shared	x	Domain 5	6.04.03. (a)	Article 4 (1), Article 12, Article 17	NIST SP 800-53 R3 RA-2	NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 AC-4		1.2.3 1.2.6 4.1.2 8.2.1 8.2.5 8.2.6		A.7.2.1	A.8.2.1		Commandment #9	General Provisions, Article 3, V. and VI.	CIP-003-3 - R4 - R5	RA-2 AC-4	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research.		PA10	SGP	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10 PCI DSS v2.0 12.3	3.1 9.6.1, 9.7.1 9.10 12.3
		DSI-01.2		Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?		No																																					
		DSI-01.3		Do you have a capability to use system geographic location as an authentication factor?		No																																					
		DSI-01.4		Can you provide the physical location/geography of storage of a tenant's data upon request?	Yes																																						
		DSI-01.5		Can you provide the physical location/geography of storage of a tenant's data in advance?	Yes																																						
		DSI-01.6		Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?		No																																					
		DSI-01.7		Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?			N/A																																				
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02	DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	Yes													APO01.06 APO03.01 APO03.02 APO09.01 APO09.01 BAI06.03 BAI09.01 BAI10.01 BAI10.02 BAI10.03 BAI10.04 BAI10.05		BOSS > Data Governance > Handling / Labeling / Security Policy			Domain 5									Clause 4.2 5.2, 7.5, 8.1						TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS					1.1.3 12.3.3
		DSI-02.2		Can you ensure that data does not migrate beyond a defined geographical residency?	Yes																																						
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes			All End User connections (End User being you, the client) are secured with HTTPS over TLS 1.2/1.1/1.0. We first attempt to secure connections using TLS 1.2, then fall back to 1.1 or 1.0, depending on what the browser is configured to support. To secure communications, we employ the use of an SSL Certificate using a 2048-bit RSA key and SHA-256 with RSA encryption certificate signature algorithm. We accept HTTP connections but immediately redirect the client to HTTPS. The Load Balancer enforces	S3.6 I13.3.a-e I3.4.0	(S3.6) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (I13.3.a-e) The procedues related to completeness, accuracy, timeliness, and authorization of system processing, including error correction and database management, are consistent with documented system processing integrity policies. (I3.4.0) The procedures related to completeness, accuracy, timeliness, and authorization of outputs are consistent with the documented system processing integrity policies.	CC5.7 PI1.5	G.4 G.11 G.16 G.18 I.3 I.4	G.19.1.1, G.19.1.2, G.19.1.3, G.10.8, G.9.11, G.14, G.15.1		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-28	COBIT 4.1 DS 5.10 5.11	APO01.06 APO03.02 APO08.01 APO13.01 APO13.02 DSS05 DSS06	312.8 and 312.10	SRM > Cryptographic Services > Data in Transit Encryption	shared	x	Domain 2		Article 17	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1	NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 SC-8 NIST SP 800-53 R3 SC-8 (1) NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1)		3.2.4 4.2.3 7.1.2 7.2.1 7.2.2 8.2.1 8.2.5	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4		Commandment #4 Commandment #5 Commandment #9 Commandment #10 Commandment #11			AC-14 AC-21 AC-22 IA-8 AU-10 SC-4 SC-8 SC-9	TR-2 SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS		PA25 PA21 PA5	GP GP BSGP	PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2	2.1.1 3.1 4.1 4.1.1 4.2
		DSI-03.2		Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes			All of MOBI's components talk together (locally) either using a keyed-hashed database or (remotely) HTTPS API. No data is communicated internally or over the Internet in an insecure fashion. Our Portal is a SaaS offering, so in a sense, yes your data is available from the Internet. All customer connections to our platform occur over HTTPS via a supported browser.																																			
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	Yes				S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1	G.13	D.2.2			DG-03	COBIT 4.1 PO 2.3, DS 11.6	APO01.06 APO03.02 APO08.01 APO09.03 APO13.01 BAI09.01 BAI09.02 BAI09.03 DSS04.07 DSS05.04 DSS05.05 DSS06.06	312.2	BOSS > Data Governance > Handling / Labeling / Security Policy	shared	x	Domain 5	6.03.05. (b)	Article 22 Article 23	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-16 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-3 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SC-9 NIST SP 800-53 R3 SC-9 (1) NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12	99.31.(a)(1)(ii)	1.1.2 5.1.0 7.1.2 8.1.0 8.2.5 8.2.6		A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1		Commandment #8 Commandment #9 Commandment #10	Chapter II Article 8, 9, 11, 12, 14, 18, 19, 20, 21	CIP-003-3 - R4 - R4.1	AC-16 MP-1 MP-3 PE-16 SI-12 SC-9	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research. SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	13.1			PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.10	9.5, 9.5.1 9.6 9.7 9.8 9.9
		DSI-04.2		Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	Yes																																						
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments.	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?		No			C3.5.0 S3.4.0 C3.21.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources. (C3.21.0) Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.	C1.3 CC5.6 C1.1		I.2.18			DG-06		APO01.06 BAI01.01 BAI03.07 BAI07.04		SRM > Policies and Standards > Technical Standard (Data Management Security Standard)	shared	x	Domain 5	6.03. (d)			NIST SP 800-53 R3 SA-11 NIST SP 800-53 R3 SA-11 (1)		1.2.6	45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.		Commandment #9 Commandment #10 Commandment #11		CIP-003-3 - R6	SA-11 CM-04	DM-1 Minimization of Personally Identifiable Information. DM-2 Data Retention & Disposal. DM-3 Minimization of PII used in Testing, Training, and Research. SE-1 INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	17.8			PCI DSS v2.0 6.4.3	6.4.3
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	Yes				S2.2.0 S2.3.0 S3.8.0	(S2.2.0) The security obligations of users and the entity's security commitments to users are communicated to authorized users. (S2.3.0) Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S3.8.0) Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary	CC2.3 CC3.1		C.2.5.1, C.2.5.2, D.1.3, L.7		Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.1.3	DG-01	COBIT 4.1 DS5.1, PO 2.3	APO01.06 APO03.02 APO13.01 APO13.03	312.4	BOSS > Data Governance > Data Ownership / Stewardship	shared	x	Domain 5		Article 4	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2		6.2.1	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	A.6.1.1 A.8.1.2 A.18.1.4		Commandment #6 Commandment #10	Chapter IV Article 30	CIP-007-3 - R1.1 - R1.2	CA-2 PM-5 PS-2 RA-2 SA-2	AP-1 AUTHORITY TO COLLECT. AP-2 PURPOSE SPECIFICATION.	3.4				3.7 12.5.5 12.10.4

Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	Yes			A senior developer will be tasked with running a script that will comb through our database and delete all data pertaining to your account. A systems administrator will login and terminate the SFTP account and delete any HR data that had been provided but not yet imported.	C3.5.0 S3.4.0	(C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies. (S3.4.0) Procedures exist to protect against unauthorized access to system resources.	C1.3 CC5.6		D.2.2.10, D.2.2.11, D.2.2.14,	37 (B)	Schedule 1 (Section 5) 4.5 - Limiting Use, Disclosure and Retention, Subsec. 4.7.5 and 4.5.3
		DSI-07.2		Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes			There is currently no public documentation that can be shared. MOBI does maintain a check list of operations to perform when a business leaves, but sharing such documentation would require exposing portions of our infrastructure that are proprietary to MOBI.							
Datacenter Security *Asset Management*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	Yes				S3.1.0 C3.14.0 S1.2.b-c	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies. (S1.2.b-c) b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction policies. c. Assessing risks on a periodic basis.	CC3.1				Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
		DCS-01.2		Do you maintain a complete inventory of all of your critical supplier relationships?	Yes						CC3.1				
Datacenter Security *Controlled Access Points*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes				A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
Datacenter Security *Equipment Identification*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	Yes				S3.2.a	(S3.2.a) a. Logical access security measures to restrict access to information resources not deemed to be public.	CC5.1	D.1	D.1.1, D.1.3		Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3
Datacenter Security *Offsite Authorization*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	Yes			There is currently no documentation around this subject. MOBI's systems reside in one location and there is currently no need to move customer data around. Should we decide to move to a new hosting vendor or location, we will be sure to inform our customers of such a change as it will definitely impact how you access our systems.	S3.2.f C3.9.0	(S3.2.f) f. Restriction of access to offline storage, backup data, systems, and media. (C3.9.0) Procedures exist to restrict physical access to the defined system including, but not limited to: facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.1 CC5.5		F.2.18, F.2.19,		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.5
Datacenter Security *Offsite equipment*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	Yes			MOBI utilizes and internal-only IT Ticket system to track assets. We are moving to a more defined asset management system that will allow us to tag and track all equipment that we issue to employees and recycle back out to other employees.	S3.4	(S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.6	D.1	D.1.1, D.2.1. D.2.2,		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.5
Datacenter Security *Policy*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Yes			Upon request, MOBI will be happy to share this information with you.	A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	H.6	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
		DCS-06.2		Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	Yes			Upon request, MOBI will be happy to share with you how we document acceptance of documented Standard Operating Proceedures.							
Datacenter Security *Secure Area Authorization*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?			N/A		A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
Datacenter Security *Unauthorized Persons Entry*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Yes			All points of entry at MOBI's office requires a valid badge to enter. The lobby is open to guests as they arrive and does not require badged entry. MOBI's NOC is located towards the rear of the office, with an entrace hidden in an embedded hallway that isn't obvious. The NOC also requires badge entry; only specific members of the IT Department have access to this room.	A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	G.21	F.2.18		Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
Datacenter Security *User Access*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	Do you restrict physical access to information assets and functions by users and support personnel?	Yes				A3.6.0	(A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	CC5.5	F.2	F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2. 9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.3, F.1.4.2, F1.4.6, F.1.4.7, F.1.6, F.1.7,F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	7 (B) 10 (B)	Schedule 1 (Section 5), 4.7 Safeguards, Subsec. 4.7.3
Encryption & Key Management *Entitlement*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Do you have key management policies binding keys to identifiable owners?	Yes										
Encryption & Key Management *Key Generation*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes			For delivery of HR data through SFTP, we can use your PGP key. However, for column-level encryption, a specific key will be unavailable. MOBI uses a very specific, strongly encrypted key for protecting the data stored in our database.		(S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.7 CC5.6		L.6	38 (B) 39 (C+)	
		EKM-02.2		Do you have a capability to manage encryption keys on behalf of tenants?		No									
		EKM-02.3		Do you maintain key management procedures?	Yes										
		EKM-02.4		Do you have documented ownership for each stage of the lifecycle of encryption keys?	Yes										
		EKM-02.5		Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	Yes										
Encryption & Key Management *Encryption*	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes				C3.12.0 S3.6.0 S3.4	(C3.12.0, S3.6.0) Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks. (S3.4) Procedures exist to protect against unauthorized access to system resources.	CC5.7 CC5.6	G.4 G.15 I.3	G.10.4, G.11.1, G.11.2, G.12.1, G.12.2, G.12.4, G.12.10, G.14.18, G.14.19, G.16.2, G.16.18, G.16.19, G.17.16, G.17.17, G.18.13, G.18.14, G.19.1.1, G.20.14	23 (B) 24 (B) 25 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3
		EKM-03.2		Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	Yes										
		EKM-03.3		Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?		No									
		EKM-03.4		Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	Yes			The MOBI Infrastructure Overview documentation outlines the use of SSL, SSH, & PGP key pairs within our organization.							
Encryption & Key Management *Storage and Access*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Yes			All encryption keys are managed by MOBI to ensure The keys are deployed separately along The Key Custodian is responsible for managing keys and securely implementing their use on our system. The Infrastructure Manager and CTO are the current Key Custodians.							
		EKM-04.2		Are your encryption keys maintained by the cloud consumer or a trusted key management provider?		No									
		EKM-04.3		Do you store encryption keys in the cloud?	Yes										
		EKM-04.4		Do you have separate key management and key usage duties?		No									
Governance and Risk Management *Baseline Requirements*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes				S1.1.0 S1.2.0(a-i)	(S1.1.0) The entity's security policies are established and periodically reviewed and approved by a designated individual or group. (S1.2.0(a-i)) The entity's security policies include, but may not be limited to, the following matters:	CC3.2	L.2	L.2, L.5, L.7 L.8, L.9, L.10	12 (B) 14 (B) 13 (B) 15 (B) 16 (C+, A+) 21 (B)	Schedule 1 (Section 5), 4.7 - Safeguards
		GRM-01.2		Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	Yes			Tests are performed each month, with PCI Compliance certification every quarter. Our compliance vendor performs both vulnerability and penetration test assessments for us. We have provided the IPs to our compliance vendor so that tests are performed on key systems of our infrastructure. We are also in the process of implementing a configuration management system to ensure the integrity of all configuration files, further ensuring the							
		GRM-01.3		Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		No		MOBI is a managed, cloud-based, SaaS offering only. Custom virtual machines will be unavailable.							
Governance and Risk Management *Risk Assessments*	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?		No		MOBI is a managed, cloud-based, SaaS offering only. Control of MOBI systems will be unavailable.	S3.1.0 C3.14.0 S1.2.b-c	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies. (S1.2.b-c) b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction policies. c. Assessing risks on a periodic basis.	CC3.1 CC3.1		L.4, L.5, L.6, L.7	34 (B)	Schedule 1 (Section 5), 4.7 - Safeguards
		GRM-02.2		Do you conduct risk assessments associated with data governance requirements at least once a year?	Yes										

Governance and Risk Management *Management Oversight*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	Yes			Yes, all managers are aware of information security and the need to follow all policies that have been developed, as well as enforcing them among their teams.	S1.2.f S2.3.0
Governance and Risk Management *Management Program*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		No		MOBI will answer any specific questions required, but does not supply documentation to customers about specific internal practices. These practices are subject to SOC audit.	x1.2.
		GRM-04.2		Do you review your Information Security Management Program (ISMP) least once a year?	Yes				
Governance and Risk Management *Management Support / Involvement*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Do you ensure your providers adhere to your information security and privacy policies?	Yes				S1.3.0
Governance and Risk Management *Policy*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	Yes			SOC 2	S1.1.0
		GRM-06.2		Do you have agreements to ensure your providers adhere to your information security and privacy policies?	Yes				
		GRM-06.3		Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or		No			S1.3.0
		GRM-06.4		Do you disclose which controls, standards, certifications and/or regulations you comply with?	Yes			PCI Compliance (Certified by SecurityMetrics) Industry Best Practices for Infrastructure HA & Security ISO27001 (MOBI's policies are developed using this framework)	S2.3.0
Governance and Risk Management *Policy Enforcement*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes				S3.9
		GRM-07.2		Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	Yes				S2.4.0
Governance and Risk Management *Business / Policy Change Impacts*	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Yes				
Governance and Risk Management *Policy Reviews*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		No			S1.1.0
		GRM-09.2		Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes				
Governance and Risk Management *Assessments*	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	Yes				S3.1
		GRM-10.2		Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	Yes				x3.1.0 S4.3.0
Governance and Risk Management *Program*	GRM-11	GRM-11.1	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.	Do you have a documented, organization-wide program in place to manage risk?	Yes				S3.1
		GRM-11.2		Do you make available documentation of your organization-wide risk management program?		No			x3.1.0
Human Resources *Asset Returns*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	Yes				S3.4
		HRS-01.2		Is your Privacy Policy aligned with industry standards?	Yes				
Human Resources *Background Screening*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	Yes				S3.11.0
Human Resources *Employment Agreements*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	Yes				S2.2.0
		HRS-03.2		Do you document employee acknowledgment of training they have completed?	Yes				
		HRS-03.3		Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	Yes				
		HRS-03.4		Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	Yes			Yes, once an employee on the Infrastructure Team (this includes Key Custodians) has been active for 90 days and completed proper training, they may submit a ticket requesting access to the servers. The process of granting access is then carried out by the Infrastructure Manager.	
		HRS-03.5		Are personnel trained and provided with awareness programs at least once a year?	Yes				
Human Resources *Employment Termination*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	Yes				S3.2.d
		HRS-04.2		Do the above procedures and guidelines account for timely revocation of access and return of assets?	Yes				S3.8.e
Human Resources *Portable / Mobile Devices*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Yes			Immediately as they are terminated. If they are leaving amicably and upon their own accord, then the user's access is typically revoked at the end of their last shift.	S3.4
Human Resources *Nondisclosure Agreements*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Yes				S4.1.0
Human Resources *Roles / Responsibilities*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?		No			S1.2.f
Human Resources *Acceptable Use*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Do you provide documentation regarding how you may or access tenant data and metadata?	Yes			Your data is stored in our database and accessed by our application. Your data is available in a similar view to our helpdesk staff so that they may support your account.	S1.2 S3.9
		HRS-08.2		Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	Yes				
		HRS-08.3		Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		No			
Human Resources *Training / Awareness*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	Yes				S1.2.k S2.2.0
		HRS-09.2		Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	Yes				
Human Resources *User Responsibility*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	Yes				S2.3.0
		HRS-10.2		Are users made aware of their responsibilities for maintaining a safe and secure working environment?	Yes				
		HRS-10.3		Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	Yes				
Human Resources *Workspace*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	Do your data management policies and procedures address tenant and service level conflicts of interests?	Yes				S3.3.0
		HRS-11.2		Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	Yes				
		HRS-11.3		Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	Yes				S3.4.0
Identity & Access Management *Audit Tools Access*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	Yes			Yes, all systems are restricted, logged, and monitored. Our system metrics are monitored via SNMP and graphed by Cacti. Our systems and services are monitored by Nagios. Logs are monitored by logwatch. Security incidents result in an immediate e-mali being sent to the Infrastructure Team's Systems Administrators. Daily logwatch reports are generated and communicate daily information from logs on all our systems to our Systems Administrators. Any	S3.2.g

		IAM-01.2		Do you monitor and log privileged access (administrator level) to information security management systems?	Yes			Yes. Four weeks of logs are kept for system services and auditing. 14 weeks of logs are kept for our applications.	
Identity & Access Management *User Access Policy*	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes				S3.2.0
		IAM-02.2		Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		No			
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Yes			All remote management is performed over the Internet using an encrypted protocol called "SSH" (Secure SHell). All systems are configured to require that a user logging in have a private and public key-pair. No users are allowed to login with plaintext passwords and each key-pair uses 2048-bit RSA encryption. Insecure DH-groups, Ciphers, and MACs have been disabled to ensure maximum protection of our remote management sessions.	S3.2.g
Identity & Access Management *Policies and Procedures*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes				
		IAM-04.2		Do you manage and store the user identity of all personnel who have network access, including their level of access?	Yes				
Identity & Access Management *Segregation of Duties*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes				S3.2.a
Identity & Access Management *Source Code Access Restriction*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	Yes				S3.13.0
		IAM-06.2		Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	Yes				
Identity & Access Management *Third Party Access*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Do you provide multi-failure disaster recovery capability?	Yes			In the event of a multi-failure, the Infrastructure Systems Administrators will work to restore systems to normal operation. Criticial systems can be restored from a snapshot. Others will need to be built and have configuration files restored (which are backed up separately of system snapshots). In the event of a singular failure, that piece will be removed, repaired, and returned to operation with minimal interruption to our customers. For a multi-failure,	S3.1 x3.1.0
		IAM-07.2		Do you monitor service continuity with upstream providers in the event of provider failure?	Yes				
		IAM-07.3		Do you have more than one provider for each service you depend on?	Yes				
		IAM-07.4		Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	Yes			If there is an incident involving an upstream provider, MOBI will generate an outage report and provide as much information as the vendor discloses to us.	
		IAM-07.5		Do you provide the tenant the ability to declare a disaster?		No			
		IAM-07.6		Do you provided a tenant-triggered failover option?		No			
		IAM-07.7		Do you share your business continuity and redundancy plans with your tenants?		No		Upon request, MOBI is happy to share the table of contents for our BCP/DR documentation.	
Identity & Access Management *User Access Restriction / Authorization*	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Do you document how you grant and approve access to tenant data?	Yes				S3.2.0 S4.3.0
		IAM-08.2		Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	Yes				
Identity & Access Management *User Access Authorization*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes				S3.2.0
		IAM-09.2		Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Yes				
Identity & Access Management *User Access Reviews*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	Yes				S3.2.0
		IAM-10.2		If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	Yes				
		IAM-10.3		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	Yes			Upon request and approval, MOBI may share this information.	
Identity & Access Management *User Access Revocation*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Yes				S3.2.0
		IAM-11.2		Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	Yes				
Identity & Access Management *User ID Credentials*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	Yes			MOBI is compatible with SAMLv2 for SSO. We can also leverage a third-party IdP such as OneLogin, Okta, Ping Federation, and Oracle.	S3.2.b
		IAM-12.2		Do you use open standards to delegate authentication capabilities to your tenants?	Yes				
		IAM-12.3		Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	Yes			MOBI is compatible with SAMLv2 for SSO. We can also leverage a third-party IdP such as OneLogin, Okta, Ping Federation, and Oracle.	
		IAM-12.4		Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	Yes			MOBI utilizes a RBAC model for managing user access.	
		IAM-12.5		Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	Yes				
		IAM-12.6		Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?		No		Only Username & Password or SSO authentication mechanisms are supported.	
		IAM-12.7		Do you allow tenants to use third-party identity assurance services?	Yes			MOBI does not provide any IdP services, so this is a customer responsibility.	
		IAM-12.8		Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	Yes				
		IAM-12.9		Do you allow tenants/customers to define password and account lockout policies for their accounts?	Yes			If custom development is requested during the sales process, MOBI can help customers extend the default MOBI Password Policy to integrate additional features requested.	

		IAM-12.10		Do you support the ability to force password changes upon first logon?	Yes			This is a base requirement for all new user accounts.	
		IAM-12.11		Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	Yes				
Identity & Access Management *Utility Programs Access*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	Yes				S3.2.g
		IAM-13.2		Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	Yes				
		IAM-13.3		Are attacks that target the virtual infrastructure prevented with technical controls?	Yes				
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	Yes				S3.7
		IVS-01.2		Is physical and logical user access to audit logs restricted to authorized personnel?	Yes			This data is only available to MOBI Infrastructure Team Systems Administrators.	
		IVS-01.3		Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?		No		This would require exposing sensitive information about our Infrastructure. Upon request, we can share limited information about security controls that are in place.	
		IVS-01.4		Are audit logs centrally stored and retained?		No		Audit logs are retained on each unique system to ensure the beach or failure of a monitoring system does not compromise the integrity of system logging or result in security data being leaked.	
		IVS-01.5		Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes			Logs are reviewed daily by the MOBI Infrastructure Team.	
Infrastructure & Virtualization Security *Change Detection*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Yes				
		IVS-02.2		Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?		No		This data is private to the Infrastructure Team.	
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes				S3.7
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?			N/A	This is not managed by MOBI.	A3.2.0
		IVS-04.2		Do you restrict use of the memory oversubscription capabilities present in the hypervisor?			N/A	This is not managed by MOBI.	A4.1.0
		IVS-04.3		Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	Yes				
		IVS-04.4		Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	Yes				
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Yes				
Infrastructure & Virtualization Security *Network Security*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			N/A	MOBI is a managed, cloud-based, SaaS offering only.	S3.4
		IVS-06.2		Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Yes				
		IVS-06.3		Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	Yes				
		IVS-06.4		Are all firewall access control lists documented with business justification?	Yes				
Infrastructure & Virtualization Security *OS Hardening and Base Conrols*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	Yes				
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?		No			S3.4
		IVS-08.2		For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			N/A		
		IVS-08.3		Do you logically and physically segregate production and non-production environments?	Yes				
Infrastructure & Virtualization Security *Segmentation*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security	Yes				S3.4
		IVS-09.2		Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	Yes				
		IVS-09.3		Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	Yes				
		IVS-09.4		Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	Yes				
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	Yes				
		IVS-10.2		Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	Yes				
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes				
Infrastructure & Virtualization Security *Wireless Security*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Yes				S3.4
		IVS-12.2		Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	Yes				
		IVS-12.3		Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes				
Infrastructure & Virtualization Security *Network Architecture*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?		No			S3.4
		IVS-13.2		Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	Yes				
Interoperability & Portability *APIs*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Yes			We are happy to share access to API with you upon signing an MSA. We currently only provide one public API for customers to use.	
Interoperability & Portability *Data Request*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	Yes				
Interoperability & Portability *Policy & Legal*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	Yes			Yes, we have complete API documentation available that we are happy to share upon signing an MSA.	
		IPY-03.2		Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Yes				
Interoperability & Portability *Standardized Network Protocols*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	Yes				
		IPY-04.2		Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?		No		No formal documentation is presented, but MOBI will answer questions if requested	
Interoperability & Portability *Virtualization*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?			N/A	MOBI is a managed, cloud-based, SaaS offering only.	
		IPY-05.2		Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?			N/A	MOBI is a managed, cloud-based, SaaS offering only.	
Mobile Security *Anti-Malware*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			N/A		
Mobile Security *Application Stores*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			N/A		
Mobile Security *Approved Applications*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?			N/A		
Mobile Security *Approved Software for BYOD*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			N/A		
Mobile Security *Awareness and Training*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			N/A		
Mobile Security *Cloud Based Services*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			N/A		
Mobile Security *Compatibility*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Do you have a documented application validation process for testing device, operating system and application compatibility issues?			N/A		

Mobile Security *Device Eligibility*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			N/A											APO01.03 APO01.08 APO13.01 APO13.02 BAI02.01		SRM > Policies and Standards > Information Security Policies	provider	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)											
Mobile Security *Device Inventory*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?			N/A	Our Portal is not mobile device friendly. Even still, all connections are secured over HTTPS. MOBI's internal policy is that all mobile devices use the Guest WiFI network so that only MOBI-certified business devices are on our coprorate network.										BAI06.01 BAI06.02 BAI06.04 BAI10.01 BAI10.02 BAI10.03		SRM > Infrastructure Protection Services > End Point - Inventory Control	provider	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3,											
Mobile Security *Device Management*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			N/A											APO03.01 APO03.02 APO04.02 APO13.01 APO13.02		Presentation Services > Presentation Platform > End-Points-Mobile	provider	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)											
Mobile Security *Encryption*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			N/A											APO01.03 APO13.01 APO13.02 DSS05.03 DSS05.05 DSS06.06		SRM > Data Protection > Cryptographic Services - Data-At-Rest Encryption	provider	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),								PA32	BSGP		4.1
Mobile Security *Jailbreaking and Rooting*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and isenforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			N/A											APO01.03 APO13.01 APO13.02 DSS05.03		Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device Management	provider	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b)											
		MOS-12.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			N/A																																					
Mobile Security *Legal*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?			N/A	All BYOD users are required to have their device inspected by the Infrastructure Team prior to using it as a business device. This ensures any laptop, phone, or tablet has the latest updates and has an auto-update setting enabled so that the latest updates are always applied.										APO01.03 APO13.01 APO13.02		SRM > Policies and Standards > Information Security Services	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1											
		MOS-13.2		Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			N/A																																					
Mobile Security *Lockout Screen*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			N/A											DSS05.03 DSS05.05		Presentation Services > Presentation Platform > End-Points-Mobile	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)											
Mobile Security *Operating Systems*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?			N/A											APO01.03 APO13.01 APO13.02 BAI06		ITOS > Service Support -Change Management > Planned Changes	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1)											
Mobile Security *Passwords*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			N/A											APO01.03 APO13.01 APO13.02 DSS05.03		Presentation Services > Presentation Platform > End-Points-Mobile Devices-Mobile Device Management	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3											
		MOS-16.2		Are your password policies enforced through technical controls (i.e. MDM)?			N/A																																					
		MOS-16.3		Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			N/A																																					
Mobile Security *Policy*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			N/A											APO01.03 APO13.01 APO13.02 DSS05.01 DSS05.03		SRM > Policies and Standards > Technical Security Standards	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3											
		MOS-17.2		Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			N/A																																					
		MOS-17.3		Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			N/A																																					
Mobile Security *Remote Wipe*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			N/A											APO01.03 APO13.01 APO13.02 DSS05.03 DSS05.05 DSS05.06		BOSS > Data Governance > Secure Disposal of Data	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3								PA34	BSGP		
		MOS-18.2		Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			N/A																																					
Mobile Security *Security Patches*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			N/A											APO01.03 APO13.01 APO13.02 DSS05.03 DSS05.05 DSS05.06		SRM > Infrastructure Protection Services- >Network > Link Layer Network Security	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3											
		MOS-19.2		Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			N/A																																					
Mobile Security *Users*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			N/A											APO01.03 APO13.01 APO13.02		SRM > Policies and Standards > Technical Security Standards	shared	X	None (Mobile Guidance)										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)											
		MOS-20.2		Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			N/A																																					
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?		No					CC3.3							APO01.01 APO01.02 APO01.03 APO01.08 MEA03.01 MEA03.02 MEA03.03	312.4	BOSS > Compliance > Contact/Authority Maintenance	shared	x										A.6.1.6 A.6.1.7	A.6.1.3 A.6.1.4			Chapter VI, Article 44. Chapter II, Article 16, part I				3.2				12.5.3 12.10.1
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Do you have a documented security incident response plan?	Yes				IS3.7.0 S3.9.0	(IS3.7.0) Procedures exist to identify, report, and act upon system security breaches and other incidents. (S3.9.0) Procedures exist to provide that issues of noncompliance with system availability, confidentiality of data, processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC5.5 CC6.2	J.1	J.1.1, J.1.2	46 (B)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.4; 4.8 Openness, Subs. 4.8.2	IS-22	COBIT 4.1 DS5.6	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	312.8 and 312.10	ITOS > Service Support > Security Incident Management	shared	x		Domain 2	6.04.07. (b) 6.07.01. (a) 6.07.01. (d) 6.07.01. (e) 6.07.01. (f) 6.07.01. (g) 6.07.01. (h)	Article 17	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-3 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8		1.2.4 1.2.7 7.1.2 7.2.2 7.2.4 10.2.1 10.2.4	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 4.3.3 A.13.1.1 A.13.2.1	Clause 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex A.16.1.1 A.16.1.2	ITAR 22 CFR § 127.12	Commandment #2 Commandment #6 Commandment #8	Chapter II, Article 20	CIP-007-3 - R6.1 CIP-008-3 - R1	IR-1 IR-2 IR-3 IR-4 IR-5 IR-7 IR-8	IP-4 COMPLAINT MANAGEMENT. SE-2 PRIVACY INCIDENT RESPONSE	4.1 4.2 4.6 7.1	PA8 PA11	BSGP	PCI-DSS v2.0 12.9 PCI-DSS v2.0 12.9.1 PCI-DSS v2.0 12.9.2 PCI-DSS v2.0 12.9.3 PCI-DSS v2.0 12.9.4 PCI-DSS v2.0 12.9.5 PCI-DSS v2.0 12.9.6	12.1
		SEF-02.2		Do you integrate customized tenant requirements into your security incident response plans?		No																																						
		SEF-02.3		Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		No																																						
		SEF-02.4		Have you tested your security incident response plans in the last year?	Yes																																							
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		No		Logs remain segregated to prevent confusion when analyzing events and for protecting log data. Log granularity still allows for in-depth analysis.	A2.3.0 C2.3.0 I2.3.0 S2.3.0 S2.4 C3.6.0	(A2.3.0, C2.3.0, I2.3.0, S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality of data, processing integrity and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them. (S2.4) The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	CC2.3 CC2.5 C1.4 C1.5	J.1 E.1	J.1.1, E.4	5 (B) 46 (B) 48 (A+) 49 (B) 50 (B)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.3	IS-23	COBIT 4.1 DS5.6	APO01.03 APO07.06 APO07.03 APO13.01 APO13.02 DSS02.01	312.3, 312.8 and 312.10	BOSS > Human Resources Security > Employee Awareness	shared	x		Domain 2	6.07.01. (a)	Article 17	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 SI-5	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-6 (1) NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 SI-4 NIST SP 800-53 R3 SI-4 (2) NIST SP 800-53 R3 SI-4 (4) NIST SP 800-53 R3 SI-4 (5) NIST SP 800-53 R3 SI-4 (6) NIST SP 800-53 R3 SI-5	99.31(a)(1)(i) 34 CFR 99.32(a)	1.2.7 1.2.10 7.1.2 7.2.2 7.2.4 10.2.4	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) (New) 16 CFR 318.5 (a) (New) 45 CFR 160.410 (a)(1) (New)	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.6.1.1 A.7.2.1, A.7.2.2, A.16.1.2, A.16.1.3, A.16.1.1	ITAR 22 CFR § 127.12	Commandment #2 Commandment #6 Commandment #8	Chapter II, Article 20	CIP-003-3 - R4.1 CIP-004-3 R3.3	IR-2 IR-6 IR-7 SI-4 SI-5	IP-4 COMPLAINT MANAGEMENT. SE-2 PRIVACY INCIDENT RESPONSE	7.2	PA8	BSGP	PCI-DSS v2.0 12.5.2 PCI-DSS v2.0 12.5.3	12.10.1
		SEF-03.2		Does your logging and monitoring framework allow isolation of an incident to specific tenants?	Yes			If a tenant's IP address is found to be producing malicious traffic, it will be immediately blocked until the tenant can address the issue on their end.																																				
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	Yes				S2.4.0 C3.15.0	(S2.4.0) The process for informing the entity about system availability issues, confidentiality issues, processing integrity issues, security issues and breaches of the system security and for submitting complaints is communicated to authorized users. (C3.15.0) Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	CC2.5 CC6.2	J.1 E.1	J.1.1, J.1.2, E.4			IS-24	COBIT 4.1 DS5.6	APO01.03 APO13.01 APO13.02 DSS01.03 DSS02.01 DSS02.02 DSS02.04 DSS02.05 DSS02.06	312.8 and 312.10	BOSS > Legal Services > Incident Response Legal Preparation	shared	x		Domain 2	6.04.07. (b) 6.07.01. (f) 6.07.01. (h)		NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-6 (1) NIST SP 800-53 R3 AU-6 (3) NIST SP 800-53 R3 AU-7 NIST SP 800-53 R3 AU-7 (1) NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-9 (2) NIST SP 800-53 R3 AU-10 NIST SP 800-53 R3 AU-10 (5) NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-7 (1) NIST SP 800-53 R3 IR-7 (2) NIST SP 800-53 R3 IR-8 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4)		1.2.7	45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.7.2.2, A.7.2.3, A.16.1.7, A.18.1.3				CIP-004-3 R3.3	AU-6 AU-7 AU-9 AU-11 IR-5 IR-7 IR-8		7.3	PA11	BSGP		
		SEF-04.2		Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	Yes																																							
		SEF-04.3		Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?		No		It is technically possible for MOBI to store point in time data for a customer and delete other customer data from that snapshot, but that would be a concierge service																																				
		SEF-04.4		Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes																																							
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	Yes				S3.9.0 C4.1.0	(S3.9.0) Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis. (C4.1.0) The entity's system security, availability, system integrity, and confidentiality is periodically reviewed and compared with the defined system security, availability, system integrity, and confidentiality policies.	CC6.2 CC4.1		J.1.2	47 (B)		IS-25	COBIT 4.1 DS 4.9	DSS04.07	312.8 and 312.10	BOSS > Operational Risk Management > Key Risk Indicators	shared	x		Domain 2	6.07.01. (a) 6.07.01. (i)		NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-4 (1) NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8		1.2.7 1.2.10	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	A.16.1.6				CIP-008-3 - R1.1	IR-4 IR-5 IR-8		7.2 7.3	PA11	BSGP	PCI DSS v2.0 12.9.6	
		SEF-05.2		Will you share statistical information for security incident data with your tenants upon request?	Yes			Upon request, If a security incident is found to directly affect a customer, an overview and debrief will be provided for review.																																				
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Yes													APO10 APO11 DSS05.04 DSS06.03 DSS06.06		SRM > Governance Risk & Compliance > Vendor Management	provider	X		Domain 2									Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),											
		STA-01.2		Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Yes																																							

Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?		No												APO09.03 APO09.04 APO10.04 APO10.05 DSS02.07		ITOS > Service Support -> Incident Management > Cross Cloud Incident Response	provider		Domain 2									Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2),											
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes				C2.2.0	(C2.2.0) The system security, availability, system integrity, and confidentiality and related security obligations of users and the entity's system security, availability, system integrity, and confidentiality and related security commitments to users are communicated to authorized users.	CC2.2 CC2.3	C.2	C.2.6, G.9.9	45 (B) 74 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-31	COBIT 4.1 DS5.10	APO01.03 APO03.01 APO03.02 APO09.03 BAI02.01 BAI02.04 BAI07.05	312.8 and 312.10	ITOS > Service Delivery > Service Level Management	provider	x	Domain 2	6.02. (c) 6.03.07. (a) 6.03.07. (b) 6.03.07. (c) 6.03.07. (d)	Article 17	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 CP-6 NIST SP 800-53 R3 CP-6 (1) NIST SP 800-53 R3 CP-6 (3) NIST SP 800-53 R3 CP-7 NIST SP 800-53 R3 CP-7 (1) NIST SP 800-53 R3 CP-7 (2) NIST SP 800-53 R3 CP-7 (3) NIST SP 800-53 R3 CP-7 (5) NIST SP 800-53 R3 CP-8 NIST SP 800-53 R3 CP-8 (1) NIST SP 800-53 R3 CP-8 (2) NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1) NIST SP 800-53 R3 SC-30		8.2.2 8.2.5		A.6.2.3 A.10.6.2	A.15.1.2 A.13.1.2		Commandment #6 Commandment #7 Commandment #8			SC-20 SC-21 SC-22 SC-23 SC-24		17.1	PA3 PA8 PA16	BSGP BSGP SGP		
		STA-03.2		Do you provide tenants with capacity planning and use reports?		No																																					
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	Yes													MEA01 MEA02		SRM > Governance Risk & Compliance > Vendor Management	provider	x	Domain 2									Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)											12.1.1
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Yes				S2.2.0 A3.6.0 C3.6.0	(S2.2.0) The availability, confidentiality of data, processing integrity, system security and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users. (A3.6.0) Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. (C3.6.0) The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.	CC2.2 CC2.3 CC5.5 C1.4 C1.5	C.2	C.2.4, C.2.6, G.4.1, G.16.3	74 (B) 75 (C+, A+) 45 (B) 75 (C+, A+) 79 (B) 4 (C+, A+)	Schedule 1 (Section 5) 4.1 Accountability, Subs. 4.1.3	LG-02	COBIT 4.1 DS5.11	APO09.03 APO09.05	312.3, 312.8 and 312.10	BOSS > Legal Services > Contracts	shared	x	Domain 3	6.02. (e) 6.10. (h) 6.10. (i)	Article 17 (3)	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 MP-5 NIST SP 800-53 R3 MP-5 (2) NIST SP 800-53 R3 MP-5 (4) NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SA-9 (1)		1.2.5		A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1	ITAR 22 CFR § 120.17 EAR 15 CFR §736.2 (b)	Commandment #1 Commandment #4 Commandment #5 Commandment #6 Commandment #7 Commandment #8	Chapter II Article 14.		CA-3 MP-5 PS-7 SA-6 SA-7 SA-9		5.2 2.2			PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2	2.4 12.8.2
		STA-05.2		Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	Yes																																						
		STA-05.3		Does legal counsel review all third-party agreements?	Yes																																						
		STA-05.4		Do third-party agreements include provision for the security and protection of information and assets?	Yes																																						
		STA-05.5		Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	Yes			MOBI will never share your data with a third-party unless previously and explicitly agreed upon with the customer.																																			
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	Yes													APO10.04 APO10.05 MEA01		SRM > Governance Risk & Compliance > Vendor Management	provider	x										Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) [illegible]											12.8.4
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	Yes									[illegible]				[illegible]		[illegible]	provider	x	Domain 2	[illegible]								[illegible]											
		STA-07.2		Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	Yes																																						
		STA-07.3		Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	Yes																																						
		STA-07.4		Do you review all agreements, policies and processes at least annually?	Yes																																						
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	Do you assure reasonable information security across your information supply chain by performing an annual review?	Yes													[illegible]		[illegible]	provider	x	Domain 2									[illegible]											
		STA-8.2		Does your annual review include all partners/third-party providers upon which your information supply chain depends?	Yes																																						
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Do you permit tenants to perform independent vulnerability assessments?		No			S3.1.0 x3.1.0	(S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats. (x3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system [availability, processing integrity, confidentiality] commitments and (2) assess the risks associated with the identified threats.	CC2.2 CC2.3 C1.4 C1.5		L.1, L.2, L.4, L.7, L.9	76 (B) 77 (B) 78 (B) 83 (B) 84 (B) 85 (B)		CO-05	COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	APO01.08 APO10.05 MEA02.01	312.2(a) and 312.3 (Prohibition on Disclosure)	BOSS > Compliance > Third-Party Audits	shared	x	Domain 2, 4	6.10. (a) 6.10. (b) 6.10. (c) 6.10. (d) 6.10. (e) 6.10. (f) 6.10. (g) 6.10. (h) 6.10. (i)		[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]		[illegible]					[illegible]	[illegible]
		STA-09.2		Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes																																						
Threat and Vulnerbility Management *Antivirus / Malicious Software*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	Yes				S3.5.0	(S3.5.0) Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	CC5.8		G.7	17 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-21	COBIT 4.1 DS5.9	APO01.03 APO13.01 APO13.02 DSS05.01	312.8 and 312.10	SRM > Infrastructure Protection Services > Anti-Virus	shared	x	Domain 2	6.03. (f)	[illegible]	[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]		[illegible]		[illegible]	[illegible]		[illegible]	[illegible]		[illegible]	[illegible]
		TVM-01.2		Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	Yes			MOBI performs daily reviews of system security, availability, and performance using three separate vectors—Cacti, Nagios, and Logwatch. Cacti allows MOBI to monitor system metrics. Nagios performs system and service checks to ensure functionality of our servers. Logwatch uses filters to comb through logs and produce a daily digest of activity occurring on the system. These three programs combined allow MOBI to assess and mitigate																																					
Threat and Vulnerbility Management *Vulnerability / Patch Management*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Yes				S3.10.0	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC7.1	I.4	G.15.2, I.3	32 (B) 33 (B)	Schedule 1 (Section 5), 4.7 - Safeguards, Subsec. 4.7.3	IS-20	COBIT 4.1 AI6.1 COBIT 4.1 AI3.3 COBIT 4.1 DS5.9	APO01.03 APO13.01 APO13.02 BAI06.01 BAI06.02 BAI06.03 BAI06.04 DSS01.01 DSS01.02 DSS01.03 DSS03.05 DSS05.01 DSS05.03 DSS05.07	312.8 and 312.10	SRM > Threat and Vulnerability Management > Vulnerability Management	shared	x	Domain 2	[illegible]		[illegible]	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]		[illegible]		[illegible]	[illegible]		[illegible]	[illegible]		[illegible]	[illegible]
		TVM-02.2		Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	Yes																																						
		TVM-02.3		Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	Yes																																						
		TVM-02.4		Will you make the results of vulnerability scans available to tenants at their request?	Yes																																						
		TVM-02.5		Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	Yes			Yes. Systems are updated monthly on the last Saturday of every month, from 8p - 2a EST. All security updates are patched within 15 days of release, or as soon as its available, depending on the severity of the CVE and whether or not it directly affects the security of MOBI's systems.																																			
		TVM-02.6		Will you provide your risk-based systems patching time frames to your tenants upon request?	Yes																																						
Threat and Vulnerbility Management *Mobile Code*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Yes			We don't allow any mobile code execution. All code executed on our systems resides in our application files. In addition, SELinux AVC policies would prevent arbitrary code from being executed.	S3.4.0 S3.10.0	(S3.4.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	CC5.6 CC7.1		G.20.12, I.2.5			SA-15		APO01.03 APO13.01 APO13.02 DSS05.01 DSS05.02 DSS05.03 DSS05.04	312.8 and 312.10	SRM > Infrastructure Protection Services > End Point - White Listing	shared	x	Domain 10	6.03. (g)	[illegible]						[illegible]	[illegible]		[illegible]			[illegible]		[illegible]				
		TVM-03.2		Is all unauthorized mobile code prevented from executing?	Yes																																						

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ) V3.0.1 GUIDING DOCUMENT

INTENT OF THIS TAB: To assist reviewers/users of document to understand both the intent and

GUIDING PRINCIPLES:

- Questionnaire is organized using CSA 16 governing & operating domains divided into “control areas” within CSA’s Controls Matrix structure

- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile

- CAIQ is not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area

- Each question should be able to be answered yes or no

- If a question can’t be answered yes or no then it was separated into two or more questions to allow yes or no answers.

- Questions are intended to foster further detailed questions to provider by client specific to client’s cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all follow-on

MA262-1
Wireless Data, Voice, and Accessories RFP
Attachment V
Category 3 Subcategory Definitions

Item	Application	Definition
A	Fleet Management	Allows the management of tasks associated with managing a fleet of vehicles through the use of telematics or remote sensing devices.
B	Mobile Device Management /Enterprise Mobility Management (MDM/EMM)	Mobile device management/enterprise mobility management (MDM/EMM) are solutions IT organizations use to manage and support end users' mobile devices, applications and data, and to enforce enterprise security policies.
C	Mobile Integration/Mobile Substitution Solutions	Network-based solutions that allow the integration of a user's mobile device and a desk phone, and provide a number of other business-oriented features. As a minimum, solutions meeting this criteria will provide: • Single Number Reach or the ability for a user to be reached at a single business telephone number. • Calls to that single telephone number would ring at both the user's desk phone or mobile device either through simultaneous and/or sequential ringing. • Single Voicemail Box for calls to that single business number.
D	Workforce Management	Workforce management solutions are systems that organizations use to manage personnel who are mobile or regularly operate outside of a fixed office or work location. Functions typically include supervisory monitoring, time and attendance tracking, enforcing pay/workforce rules, scheduling, planning , task management, capacity planning, budgeting, forecasting, and other related functions
E	Field Service Management	Systems that support the management of field service operations typically managing service orders, dispatching technicians, work planning, route optimization, time recording, maintenance data collection/analysis and other related functions.

F	Mobile Data Collection/Mobile Forms	A solution(s) that allow mobile users with cellular-equipped tablets or smartphones to collect data and possibly other information (e.g. pictures, videos, audio notes, locations, etc.), which is then sent over the cellular network to a cloud storage facility from which it can be accessed or downloaded by the customer.
G	Traffic Management and Intelligent Transport Systems (ITS)	Systems implemented by local governments to manage the flow of vehicle and potentially pedestrian traffic to reduce congestion, improve efficiency, reduce energy waste, improve safety and optimize road utilization.
H	Snow & Ice Removal and Route Management	Systems that would be used by government (and potentially other) agencies to manage road clearing operations resulting from snow storms or other weather events. Functions might include vehicle location, monitoring road conditions, dispatch, materials management, time clock, workforce monitoring, reporting, and other related functions.
I	Public Safety Systems	Any system that would be used by public safety organizations (e.g. Police, Fire, EMS, etc.) in executing their duties. Those functions might include multimodal communications, locating resources, managing responses, routing and dispatching, building and site intelligence, ongoing monitoring and detection systems, and other related functions.
J	IoT Management	Solutions to monitor, manage and maintain networks of Internet of Things (IoT) devices. Functions might include maintaining inventory, monitoring health/performance, measuring utilization, security maintenance, diagnostics and troubleshooting, downloading software/firmware updates, executing remote commands (e.g. turn off/on, reboot, etc.), logging/reporting, and other related functions.
K	Energy Conservation/ Management	Systems that optimizes the operation of the heating, cooling, lighting and other energy consuming systems within buildings enabling building owners to track energy usage, improve energy conservation, and manage energy economics and sustainability compliance.
L	Building & Facilities Automation	Similar to Energy Conservation/Management but focused on a wider range of systems including building access, security, and other functions to improve occupant comfort and security, ensure efficient operation of building systems, reduction in energy consumption and operating costs, and improve the life cycle of building utilities.
M	Enterprise Messaging	A messaging solution offered as an alternative to traditional SMS/MMS and offering enterprise-grade security, archiving, and retrieval geared for the messaging requirements of organizations with stringent security requirements.
N	Secure LAN Access	A cellular wireless service providing a secure end-to-end virtual private network (VPN) type connection between a mobile device and to the customer's local area network (LAN).

NASPO ValuePoint

MA262-1

Attachment W

Wireless Data, Voice and Accessories RFP

Offeror Submission Sheet

Offeror Name: Sprint

Category (subcategory)	Yes	No	Regional Award?
Category 1: Wireless Voice and Data	X		N/A
Category 2: Wireless Accessories and Equipment	X		N/A
Category 3: Turnkey Wireless Solutions (Check this if any subcategories below)	X		
Category 3: Subcategory A: Fleet Management	X		
Category 3: Subcategory B: Mobile Device Management/Enterprise Mobility (MDM/EMM)		X	
Category 3: Subcategory C: Mobile Integration/Mobile Substitution Solutions		X	
Category 3: Subcategory D: Workforce Management		X	
Category 3: Subcategory E: Field Service Management		X	
Category 3: Subcategory F: Mobile Data Collection/Mobile Forms	X		
Category 3: Subcategory G: Traffic Management and Intelligent Transport Systems (ITS)		X	
Category 3: Subcategory H: Snow and Ice Removal Route Management		X	
Category 3: Subcategory I: Public Safety Systems		X	
Category 3: Subcategory J: IoT Management		X	
Category 3: Subcategory K: Energy Conservation/Management		X	
Category 3: Subcategory L: Building and Facilities Automation		X	
Category 3: Subcategory M: Enterprise Messaging	X		
Category 3: Subcategory N: Secure LAN Access	X		
Category 4: Alternate Data Transport		X	