# CAIQ Compliance

| Category | Question | Yes | Code | Description |
|---|---|---|---|---|
| Application & Interface Security | Do you use industry standards (BuildSecurityin Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build inSecurityfor your Systems/SoftwareDevelopmentLifecycle (SDLC)? | X | | (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined systemSecuritypolicies to enable authorized access and to prevent unauthorized access. |
| Application Security | Do you use an automated source code analysis tool to detectSecuritydefects in code prior to production? | X | S3.10.0 | (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and relatedSecuritypolicies. |
| | Do you use manual source-code analysis to detectSecuritydefects in code prior to production? | X | | |
| | Do you verify that all of your software suppliers adhere to industry standards for Systems/SoftwareDevelopmentLifecycle (SDLC) security? | X | | |
| | (SaaS only) Do you review your applications forSecurityvulnerabilities and address any issues prior to deployment to production? | | | |
| Application & Interface Security | 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 | S3.2a | (S3.2.a) a. Logical accessSecuritymeasures to restrict access to information resources not deemed to be public. |
| Customer Access Requirements | Are all requirements and trust levels for customers' access defined and documented? | X | | |
| Application & Interface Security | | | S3.4 | (I3.2.0) The procedures related to completeness, accuracy, timeliness, and authorization of inputs are consistent with the documented system processing integrity policies. |
| 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? | | | (I3.3.0) The procedures 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. |
| | | | | (I3.5.0) There are procedures to enable tracing of information inputs from their source to their final disposition and vice versa. |
| Application & Interface Security | Is your DataSecurityArchitecturedesigned using an industry standard (e.g., CDSA, MULITSAFE, CSA TrustedCloudArchitectural Standard, FedRAMP, CAESARS)? | X | | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| Data Security / Integrity | | | | |
| **Audit Assurance &Compliance** | | | S4.1.0 | (S4.1.0) The entity’s systemSecurityis periodically reviewed and compared with the defined systemSecuritypolicies. |
| | Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA'sCloudComputing Management Audit/Assurance Program, etc.)? | | | |
| Audit Planning | | | | |
| | | | | (S4.2.0) There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined systemSecuritypolicies. |

| | | | | |
|---|---|---|---|---|
| | | | S4.2.0 | |
| Audit Assurance &Compliance | Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports? | Yes | S4.1.0 | (S4.1.0) The entity’s systemSecurityis periodically reviewed and compared with the defined systemSecuritypolicies. |
| Independent Audits | Do you conduct network penetration tests of yourCloudservice infrastructure regularly as prescribed by industry best practices and guidance? | Yes | | |
| | Do you conduct application penetration tests of yourCloudinfrastructure regularly as prescribed by industry best practices and guidance? | Yes | | (S4.2.0) There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined systemSecuritypolicies. |
| | Do you conduct internal audits regularly as prescribed by industry best practices and guidance? | Yes | | |
| | | | S4.2.0 | |
| | Do you conduct external audits regularly as prescribed by industry best practices and guidance? | Yes | | |
| | Are the results of the penetration tests available to tenants at their request? | | | |
| | Are the results of internal and external audits available to tenants at their request? | Yes | | |
| | Do you have an internal audit program that allows for cross-functional audit of assessments? | Yes | | |
| Audit Assurance &Compliance | 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? | | | |
| Information System Regulatory Mapping | Do you have capability to recover data for a specific customer in the case of a failure or data loss? | | | |
| | Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? | | | |
| | Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust yourSecurityprogram for changes to legal requirements, and ensureCompliancewith relevant regulatory requirements? | Yes | | |
| Business Continuity Management & Operational Resilience | Do you provide tenants with geographically resilientHostingoptions? | Yes | A3.1.0 | (A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. |
| Business Continuity Planning | | | | |

| | | | | |
|---|---|---|---|---|
| | | | A3.3.0 | (A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity’s defined system availability and relatedSecuritypolicies. |
| | Do you provide tenants with infrastructure service failover capability to other providers? | Yes | A3.4.0 | (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 relatedSecuritypolicies. |
| Business Continuity Management & Operational Resilience | Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? | Yes | A3.3 | (A3.3) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity’s defined system availability and relatedSecuritypolicies. |
| **Business ContinuityTesting** | | | | |
| Business Continuity Management & Operational Resilience<br>Power / Telecommunications | Do you provide tenants with documentation showing the transport route of their data between your systems? | | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| | Can tenants define how their data is transported and through which legal jurisdictions? | | A3.4.0 | (A3.4.0) Procedures exist to protect against unauthorized access to system resource. |

| | | | | |
|---|---|---|---|---|
| Business Continuity Management & Operational Resilience<br>Documentation | Are information system documents (e.g., administrator and user guides,Architecturediagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system? | Yes | S3.11.0 | (S3.11.0) Procedures exist to provide that personnel responsible for the design,Development, implementation, and operation of systems affectingSecurityhave the qualifications and resources to fulfill their responsibilities. |
| | | | A.2.1.0 | (A.2.1.0) The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users. |
| Business Continuity Management & Operational Resilience<br>Environmental Risks | Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied? | Yes | A3.1.0 | (A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. |
| | | | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| Business Continuity Management & Operational Resilience<br>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.)? | | A3.1.0 | (A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. |
| | | | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| Business Continuity Management & Operational Resilience | If using virtual infrastructure, does yourCloudsolution include independent hardware restore and recoverycapabilities? | Yes | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| Equipment Maintenance | If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time? | Yes | | |

| | | | | |
|---|---|---|---|---|
| | If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a newCloudprovider? | Yes | | (A4.1.0) The entity’s system availability andSecurityperformance is periodically reviewed and compared with the defined system availability and relatedSecuritypolicies. |
| | 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? | Yes | | |
| | Does yourCloudsolution include software/provider independent restore and recoverycapabilities? | Yes | A4.1.0 | |
| Business Continuity Management & Operational Resilience | AreSecuritymechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? | Yes | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| Equipment Power Failures | | | | |
| Business Continuity Management & Operational Resilience | | | A3.1.0 | (A3.1.0) Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats. |
| Impact Analysis | Do you provide tenants with ongoing visibility andReportingof your operational Service Level Agreement (SLA) performance? | | | |
| | | | | (A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity’s defined system availability and relatedSecuritypolicies. |
| | | | A3.3.0 | |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | (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 relatedSecuritypolicies. |
|  | Do you make standards-based informationSecuritymetrics (CSA, CAMM, etc.) available to your tenants? |  |  |  |
|  | Do you provide customers with ongoing visibility andReportingof your SLA performance? |  | A3.4.0 |  |
| Business Continuity Management & Operational Resilience | 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, systemSecurityand relatedSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |
| Policy |  |  |  |  |

| | | | | |
|---|---|---|---|---|
| Business Continuity Management & Operational Resilience | | | A3.3.0 | (A3.3.0) Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity’s defined system availability and relatedSecuritypolicies. |
| Retention Policy | | | | |
| | Do you have technical controlcapabilitiesto enforce tenant data retention 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 relatedSecuritypolicies. |
| | | | | (I3.20.0) Procedures exist to provide for restoration and disaster recovery consistent with the entity’s defined processing integrity policies. |
| | | | A3.4.0 | |
| | | | | (I3.21.0) Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems. |
| | | | I3.20.0 | |
| | Do you have a documented procedure for responding to requests for tenant data from governments or third parties? | Yes | | |
| | Have you implemented backup or redundancy mechanisms to ensureCompliancewith regulatory, statutory, contractual or business requirements? | Yes | | |
| | Do you test your backup or redundancy mechanisms at least annually? | Yes | I3.21.0 | |
| Change Control & Configuration Management | | | S3.12.0 | (S3.12.0) Procedures exist to maintain system components, including configurations consistent with the defined systemSecuritypolicies. |
| **NewDevelopment/ Acquisition** | Are policies and procedures established for management authorization forDevelopmentor acquisition of new applications, systems, databases, infrastructure, services, operations and facilities? | Yes | | |
| | | | | (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined systemSecuritypolicies. |

| | | | | |
|---|---|---|---|---|
| | | | S3.10.0 | (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system. |
| | Is documentation available that describes the installation, configuration and use of products/services/features? | Yes | S3.13.0 | |
| Change Control & Configuration Management | | | S3.10.0 | (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, systemsSecurityand relatedSecuritypolicies. |
| OutsourcedDevelopment | Do you have controls in place to ensure that standards of quality are being met for all softwareDevelopment? | | | |
| | | | | (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system. |
| | Do you have controls in place to detect source codeSecuritydefects for any outsourced softwareDevelopmentactivities? | | S3.13 | |
| Change Control & ConfigurationManagement | | | A3.13.0 | (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, systemsSecurityand relatedSecuritypolicies. |
| | Do you provide your tenants with documentation that describes your quality assurance process? | | | |
| QualityTesting | | | C3.16.0 | |
| | | | I3.14.0 | (S3.13) Procedures exist to provide that only authorized, tested, and documented changes are made to the system. |
| | | | S3.10.0 | |
| | Is documentation describing known issues with certain products/services available? | | | |
| | Are there policies and procedures in place to triage and remedy reported bugs andSecurityvulnerabilities for product and service offerings? | Yes | | |

|  |  |  |  |  |
|---|---|---|---|---|
|  | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? |  | S3.13 |  |
| Change Control & Configuration Management |  |  | 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. |
| Unauthorized Software Installations |  |  |  |  |
|  | Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | Yes |  | (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. |
|  |  |  | S3.5.0 |  |
|  |  |  | S3.13.0 |  |
| Change Control & Configuration Management | Do you provide tenants with documentation that describes your production change management procedures and theirRoles/rights/responsibilities within it? | Yes | A3.16.0 | (A3.16.0, S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system. |
| Production Changes |  |  | S3.13.0 |  |

| | | | | |
|---|---|---|---|---|
| Data Security & Information Lifecycle Management | 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)? | Yes | S3.8.0 | (S3.8.0) Procedures exist to classify data in accordance withClassificationpolicies and periodically monitor and update such classifications as necessary. |
| Classification | Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? | Yes | | |
| | Do you have a capability to use system geographic location as anAuthenticationfactor? | | | (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and relatedSecuritypolicies. |
| | Can you provide the physical location/geography of storage of a tenant’s data upon request? | Yes | | |
| | Can you provide the physical location/geography of storage of a tenant's data in advance? | | C3.14.0 | |
| | Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | | | |
| | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | Yes | | |
| Data Security & Information Lifecycle Management | 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? | | | |
| Data Inventory / Flows | Can you ensure that data does not migrate beyond a defined geographical residency? | | | |
| Data Security & Information Lifecycle Management | | | S3.6 | (S3.6) Encryption or other equivalentSecuritytechniques are used to protect transmissions of userAuthenticationand other confidential information passed over the Internet or other public networks. |
| 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)? | | | (I13.3.a-e) The procedures 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. |
| | | | I13.3.a-e | |

|  |  |  |  |  |
|---|---|---|---|---|
|  | 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 | I3.4.0 |  |
| Data Security & Information Lifecycle Management | Are policies and procedures established for labeling, handling and theSecurityof data and objects that contain data? | Yes | S3.2.a | (S3.2.a) a. Logical accessSecuritymeasures to restrict access to information resources not deemed to be public. |
| **Handling / Labeling /SecurityPolicy** | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? |  |  |  |
| Data Security & Information Lifecycle Management |  |  | C3.5.0 | (C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and relatedSecuritypolicies. |
| Nonproduction Data |  |  |  |  |
|  |  |  |  | (S3.4.0) Procedures exist to protect against unauthorized access to system resources. |
|  | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | Yes |  |  |
|  |  |  | S3.4.0 | (C3.21.0) Procedures exist to provide that confidential information is protected during the systemDevelopment,Testing, and change processes in accordance with defined system confidentiality and relatedSecuritypolicies. |
|  |  |  | C3.21.0 |  |
| Data Security & Information Lifecycle Management |  |  | S2.2.0 | (S2.2.0) TheSecurityobligations of users and the entity'sSecuritycommitments to users are communicated to authorized users. |
| Ownership / Stewardship |  |  |  |  |
|  | Are the responsibilities regarding data stewardship defined, assigned, documented and communicated? | Yes |  |  |
|  |  |  |  | (S2.3.0) Responsibility and accountability for the entity's systemSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |

| | | | | |
|---|---|---|---|---|
| | | | S2.3.0 | (S3.8.0) Procedures exist to classify data in accordance withClassificationpolicies and periodically monitor and update such classifications as necessary |
| | | | S3.8.0 | |
| Data Security & Information Lifecycle Management | | | C3.5.0 | (C3.5.0) The system procedures provide that confidential information is disclosed to parties only in accordance with the entity’s defined confidentiality and relatedSecuritypolicies. |
| | Do you supportsecuredeletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant? | | | |
| **secureDisposal** | | | | |
| | | | | (S3.4.0) Procedures exist to protect against unauthorized access to system resources. |
| | 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 | S3.4.0 | |
| Datacenter Security | | | S3.1.0 | (S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| Asset Management | | | | |
| | | | | (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and relatedSecuritypolicies. |
| | Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset? | Yes | | |
| | | | | (S1.2.b-c) b.Classifyingdata based on its criticality and sensitivity and thatClassificationis used to define protection requirements, access rights and access restrictions, and retention and destruction policies. |
| | | | C3.14.0 | c. Assessing risks on a periodic basis. |

| | | | | |
|---|---|---|---|---|
| | Do you maintain a complete inventory of all of your critical supplier relationships? | Yes | S1.2.b-c | |
| Datacenter Security | Are physicalSecurityperimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physicalAuthenticationmechanisms, reception desks andSecuritypatrols) 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. |
| Controlled Access Points | | | | |
| Datacenter Security | Is automated equipment identification used as a method to validate connectionAuthenticationintegrity based on known equipment location? | Yes | S3.2.a | (S3.2.a) a. Logical accessSecuritymeasures to restrict access to information resources not deemed to be public. |
| Equipment Identification | | | | |
| Datacenter Security | 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 | S3.2.f | (S3.2.f) f. Restriction of access to offline storage, backup data, systems, and media. |
| Offsite Authorization | | | | |

| | | | | |
|---|---|---|---|---|
| | | | C3.9.0 | (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. |
| Datacenter Security | Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment? | Yes | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| Offsite equipment | | | | |
| Datacenter Security | Can you provide evidence that policies, standards and procedures have been established for maintaining a safe andsecureworking environment in offices, rooms, facilities andsecureareas? | 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. |
| Policy | Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures? | Yes | | |

| | | | | |
|---|---|---|---|---|
| Datacenter Security | 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)? | | 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. |
| **secureArea Authorization** | | | | |
| Datacenter Security | 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 | 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. |
| Unauthorized Persons Entry | | | | |

|  |  |  |  |  |
|---|---|---|---|---|
| Datacenter Security | 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. |
| User Access |  |  |  |  |
| Encryption & Key Management | Do you have key management policies binding keys to identifiable owners? |  |  |  |
| Entitlement |  |  |  |  |
| Encryption & Key Management | Do you have a capability to allow creation of unique encryption keys per tenant? |  |  | (S3.6.0) Encryption or other equivalentSecuritytechniques are used to protect transmissions of userAuthenticationand other confidential information passed over the Internet or other public networks. |
| Key Generation | Do you have a capability to manage encryption keys on behalf of tenants? |  |  |  |
|  | Do you maintain key management procedures? |  |  | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
|  | Do you have documented ownership for each stage of the lifecycle of encryption keys? |  |  |  |
|  | Do you utilize any third party/open source/proprietary frameworks to manage encryption keys? |  |  |  |

| | | | | |
|---|---|---|---|---|
| Encryption & Key Management | | | C3.12.0 | (C3.12.0, S3.6.0) Encryption or other equivalentSecuritytechniques are used to protect transmissions of userAuthenticationand other confidential information passed over the Internet or other public networks. |
| | Do you encrypt tenant data at rest (on disk/storage) within your environment? | | | |
| Encryption | | | S3.6.0 | |
| | | | | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| | Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances? | | | |
| | 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)? | Yes | | |
| | Do you have documentation establishing and defining your encryption management policies, procedures and guidelines? | | S3.4 | |
| Encryption & Key Management | Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms? | | | |
| Storage and Access | Are your encryption keys maintained by theCloudconsumer or a trusted key management provider? | | | |
| | Do you store encryption keys in theCloud? | | | |
| | Do you have separate key management and key usage duties? | | | |
| Governance and Risk Management | | | S1.1.0 | (S1.1.0) The entity’sSecuritypolicies are established and periodically reviewed and approved by a designated individual or group. |
| Baseline Requirements | Do you have documented informationSecuritybaselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? | Yes | | |
| | | | | (S1.2.0(a-i)) The entity'sSecuritypolicies include, but may not be limited to, the following matters: |
| | Do you have a capability to continuously monitor and report theComplianceof your infrastructure against your informationSecuritybaselines? | Yes | | |
| | Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards? | Yes | S1.2.0(a-i) | |
| Governance and Risk Management | Do you provideSecuritycontrol 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)? | | S3.1.0 | (S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| Risk Assessments | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | (C3.14.0) Procedures exist to provide that system data are classified in accordance with the defined confidentiality and relatedSecuritypolicies. |
| | | | | (S1.2.b-c) b.Classifyingdata based on its criticality and sensitivity and thatClassificationis used to define protection requirements, access rights and access restrictions, and retention and destruction policies. |
| | | | C3.14.0 | c. Assessing risks on a periodic basis. |
| | Do you conduct risk assessments associated with data governance requirements at least once a year? | Yes | S1.2.b-c | |
| Governance and Risk Management | | | S1.2.f | (S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security. |
| Management Oversight | Are your technical, business, and executive managers responsible for maintaining awareness of andCompliancewithSecuritypolicies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility? | Yes | | (S2.3.0) Responsibility and accountability for the entity's systemSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |
| | | | S2.3.0 | |
| Governance and Risk Management | Do you provide tenants with documentation describing your InformationSecurityManagement Program (ISMP)? | Yes | x1.2. | (x1.2.) The entity's system [availability, processing integrity, confidentiality and related]Securitypolicies include, but may not be limited to, the following matters: |
| Management Program | Do you review your InformationSecurityManagement Program (ISMP) least once a year? | Yes | | |
| Governance and Risk Management | | | | (S1.3.0) Responsibility and accountability for developing and maintaining the entity's systemSecuritypolicies, and changes andUpdatesto those policies, are assigned. |
| Management Support / Involvement | Do you ensure your providers adhere to your informationSecurityand privacy policies? | Yes | S1.3.0 | |
| | | | | The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users |

| | | | | |
|---|---|---|---|---|
| | | | | TheSecurityobligations of users and the entity’sSecuritycommitments to users are communicated to authorized users. |
| Governance and Risk Management | | | S1.1.0 | (S1.1.0) The entity'sSecuritypolicies are established and periodically reviewed and approved by a designated individual or group. |
| Policy | | | | |
| | Do your informationSecurityand privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? | Yes | | (S1.3.0) Responsibility and accountability for developing and maintaining the entity’s systemSecuritypolicies, and changes andUpdatesto those policies, are assigned. |
| | | | S1.3.0 | (S2.3.0) Responsibility and accountability for the entity's systemSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |
| | Do you have agreements to ensure your providers adhere to your informationSecurityand privacy policies? | Yes | | |
| | Can you provide evidence of due diligence mapping of your controls,Architectureand processes to regulations and/or standards? | Yes | | |
| | Do you disclose which controls, standards, certifications and/or regulations you comply with? | Yes | S2.3.0 | |
| Governance and Risk Management | | | S3.9 | (S3.9) Procedures exist to provide that issues of noncompliance withSecuritypolicies are promptly addressed and that corrective measures are taken on a timely basis. |
| Policy Enforcement | Is a formal disciplinary or sanction policy established for employees who have violatedSecuritypolicies and procedures? | Yes | | |
| | | | | (S2.4.0) TheSecurityobligations of users and the entity’sSecuritycommitments to users are communicated to authorized users. |
| | 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 | Do risk assessment results includeUpdatestoSecuritypolicies, procedures, standards and controls to ensure they remain relevant and effective? | Yes |  |  |
| Business / Policy Change Impacts |  |  |  |  |
| Governance and Risk Management | Do you notify your tenants when you make material changes to your informationSecurityand/or privacy policies? | Yes | S1.1.0 | (S1.1.0) The entity’sSecuritypolicies are established and periodically reviewed and approved by a designated individual or group. |
| Policy Reviews | Do you perform, at minimum, annual reviews to your privacy andSecuritypolicies? | Yes |  |  |
| Governance and Risk Management |  |  | S3.1 | (S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| 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 identified risks, using qualitative and quantitative methods? | Yes | x3.1.0 | (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.<br>(S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality of data, processing integrity, and systemSecurityis assessed on a timely basis; policies are updated for that assessment. |

| | | | | |
|---|---|---|---|---|
| | 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 regulatoryCompliance)? | Yes | S4.3.0 | |
| Governance and Risk Management | | | S3.1 | (S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| Program | | | | |
| | Do you have a documented, organization-wide program in place to manage risk? | Yes | | (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. |
| | Do you make available documentation of your organization-wide risk management program? | Yes | x3.1.0 | |
| Human Resources | Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data? | | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| Asset Returns | Is your Privacy Policy aligned with industry standards? | Yes | | |

| | | | | |
|---|---|---|---|---|
| Human Resources | 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 | (S3.11.0) Procedures exist to help ensure that personnel responsible for the design,Development, implementation, and operation of systems affecting confidentiality andSecurityhave the qualifications and resources to fulfill their responsibilities. |
| Background Screening | | | | |
| Human Resources | Do you specifically train your employees regarding their specific role and the informationSecuritycontrols they must fulfill? | Yes | | |
| Employment Agreements | Do you document employee acknowledgment of training they have completed? | Yes | | |
| | Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information? | Yes | S2.2.0 | (S2.2.0) TheSecurityobligations of users and the entity'sSecuritycommitments to users are communicated to authorized users |
| | Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems? | Yes | | |
| | Are personnel trained and provided with awareness programs at least once a year? | Yes | | |
| Human Resources | | | S3.2.d | (S3.2.d) Procedures exist to restrict logical access to the system and information resources maintained in the system including, but not limited to, the following matters: |
| | Are documented policies, procedures and guidelines in place to govern change in employment and/or termination? | Yes | | |
| Employment Termination | | | | d. The process to make changes andUpdatesto user profiles |

| | | | | |
|---|---|---|---|---|
| | | | | (S3.8.e) e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own |
| | Do the above procedures and guidelines account for timely revocation of access and return of assets? | Yes | S3.8.e | |
| Human Resources | 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 | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| Portable / Mobile Devices | | | | |

| | | | | |
|---|---|---|---|---|
| Human Resources | 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 | (S4.1.0) The entity’s system availability, confidentiality, processing integrity andSecurityperformance is periodically reviewed and compared with the defined system availability and relatedSecuritypolicies. |
| Nondisclosure Agreements | | | | |
| Human Resources | Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? | Yes | S1.2.f | (S1.2.f) f. Assigning responsibility and accountability for system availability, confidentiality, processing integrity and related security. |
| **Roles/ Responsibilities** | | | | |
| Human Resources | Do you provide documentation regarding how you may or access tenant data and metadata? | | S1.2 | (S1.2) The entity’sSecuritypolicies include, but may not be limited to, the following matters: |
| Acceptable Use | | | | |
| | Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)? | | | (S3.9) Procedures exist to provide that issues of noncompliance withSecuritypolicies are promptly addressed and that corrective measures are taken on a timely basis. |
| | Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? | | S3.9 | |

| | | | | |
|---|---|---|---|---|
| Human Resources | | | S1.2.k | (S1.2.k) The entity'sSecuritypolicies include, but may not be limited to, the following matters: |
| Training / Awareness | Do you provide a formal, role-based,Securityawareness training program forCloud-related access and data management issues (e.g., multi-tenancy, nationality,Clouddelivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data? | Yes | | k. Providing for training and other resources to support its systemSecuritypolicies |
| | | | | (S2.2.0) TheSecurityobligations of users and the entity'sSecuritycommitments to users are communicated to authorized users. |
| | Are administrators and data stewards properly educated on their legal responsibilities with regard toSecurityand data integrity? | Yes | S2.2.0 | |
| Human Resources | Are users made aware of their responsibilities for maintaining awareness andCompliancewith publishedSecuritypolicies, procedures, standards and applicable regulatory requirements? | Yes | S2.3.0 | (S2.3.0) Responsibility and accountability for the entity's system availability, confidentiality, processing integrity andSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |
| User Responsibility | Are users made aware of their responsibilities for maintaining a safe andsecureworking environment? | Yes | | |
| | Are users made aware of their responsibilities for leaving unattended equipment in asecuremanner? | Yes | | |
| Human Resources | | | S3.3.0 | (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. |
| | Do your data management policies and procedures address tenant and service level conflicts of interests? | Yes | | |
| Workspace | | | | |
| | | | | (S3.4.0) Procedures exist to protect against unauthorized access to system resources. |
| | Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data? | | | |
| | 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? | | S3.4.0 | |
| Identity & Access Management | Do you restrict, log and monitor access to your informationSecuritymanagement systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) | Yes | S3.2.g | (S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Audit Tools Access | Do you monitor and log privileged access (administrator level) to informationSecuritymanagement systems? | Yes | | |
| Identity & Access Management | | | | (S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: |
| | Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? | Yes | S3.2.0 | |
| User Access Policy | | | | c. Registration and authorization of new users. |

| | | | | |
|---|---|---|---|---|
| | | | | d. The process to make changes to user profiles. |
| | 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? | Yes | | g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Identity & Access Management | Do you use dedicatedsecurenetworks to provide management access to yourCloudservice infrastructure? | Yes | S3.2.g | (S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Diagnostic / Configuration Ports Access | | | | |
| Identity & Access Management | Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? | Yes | | |
| Policies and Procedures | Do you manage and store the user identity of all personnel who have network access, including their level of access? | Yes | | |

| | | | | |
|---|---|---|---|---|
| Identity & Access Management | Do you provide tenants with documentation on how you maintain segregation of duties within yourCloudservice offering? | Yes | S3.2.a | (S3.2.a) a. Logical accessSecuritymeasures to restrict access to information resources not deemed to be public. |
| Segregation of Duties | | | | |
| Identity & Access Management | 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 | (S3.13.0) Procedures exist to provide that only authorized, tested, and documented changes are made to the system. |
| 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 authorized personnel only? | Yes | | |
| Identity & Access Management | Do you provide multi-failure disaster recovery capability? | Yes | S3.1 | (S3.1) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| Third Party Access | Do you monitor service continuity with upstream providers in the event of provider failure? | Yes | | |
| | Do you have more than one provider for each service you depend on? | Yes | | (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. |
| | Do you provide access to operational redundancy and continuity summaries, including the services you depend on? | Yes | | |
| | Do you provide the tenant the ability to declare a disaster? | | | |
| | Do you provided a tenant-triggered failover option? | | x3.1.0 | |
| | Do you share your business continuity and redundancy plans with your tenants? | Yes | | |
| Identity & Access Management | | | S3.2.0 | (S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: |
| User Access Restriction / Authorization | Do you document how you grant and approve access to tenant data? | | | c. Registration and authorization of new users.<br>d. The process to make changes to user profiles. |

| | | | | |
|---|---|---|---|---|
| | | | | g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| | | | | (S4.3.0) Environmental, regulatory, and technological changes are monitored, and their effect on system availability, confidentiality, processing integrity andSecurityis assessed on a timely basis; policies are updated for that assessment. |
| | Do you have a method of aligning provider and tenant dataClassificationmethodologies for access control purposes? | | S4.3.0 | |
| Identity & Access Management | 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 | (S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: |
| User Access Authorization | | | | c. Registration and authorization of new users. |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | d. The process to make changes to user profiles. |
|  | 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 |  | g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Identity & Access Management | 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) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: |
| User Access Reviews | If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? | Yes | S3.2.0 | d. The process to make changes to user profiles. |
|  | Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data? | Yes |  | g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Identity & Access Management | 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 | (S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: |
| User Access Revocation |  |  |  | d. The process to make changes to user profiles. |

| | | | | |
|---|---|---|---|---|
| | 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 | | g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| Identity & Access Management | Do you support use of, orIntegrationwith, existing customer-based Single Sign On (SSO) solutions to your service? | | | |
| User ID Credentials | Do you use open standards to delegateAuthenticationcapabilitiesto your tenants? | | | |
| | Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? | | | |
| | Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access? | | | |
| | Do you have an identity management system (enablingClassificationof data for a tenant) in place to enable both role-based and context-based entitlement to data? | | | |
| | Do you provide tenants with strong (multifactor)Authenticationoptions (digital certs, tokens, biometrics, etc.) for user access? | | S3.2.b | (S3.2.b) b. Identification andAuthenticationof users. |
| | Do you allow tenants to use third-party identity assurance services? | Yes | | |
| | Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement? | Yes | | |
| | Do you allow tenants/customers to define password and account lockout policies for their accounts? | Yes | | |
| | Do you support the ability to force password changes upon first logon? | Yes | | |
| | Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service viaEmail, defined challenge questions, manual unlock)? | Yes | | |
| Identity & Access Management | Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored? | Yes | | |
| 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.)? | Yes | S3.2.g | (S3.2.g) g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, andSecuritydevices (for example, firewalls). |
| | Are attacks that target the virtual infrastructure prevented with technical controls? | Yes | | |
| Infrastructure & Virtualization Security | 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 | | |
| Audit Logging / Intrusion Detection | Is physical and logical user access to audit logs restricted to authorized personnel? | Yes | S3.7 | (S3.7) Procedures exist to identify, report, and act upon systemSecuritybreaches and other incidents. |
| | Can you provide evidence that due diligence mapping of regulations and standards to your controls/Architecture/processes has been done? | Yes | | |
| | Are audit logs centrally stored and retained? | Yes | | |

| | | | | |
|---|---|---|---|---|
| | Are audit logs reviewed on a regular basis forSecurityevents (e.g., with automated tools)? | Yes | | |
| Infrastructure & Virtualization Security | Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? | | | |
| 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)? | Yes | | |
| Infrastructure & Virtualization Security | Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? | Yes | S3.7 | (S3.7) Procedures exist to identify, report, and act upon systemSecuritybreaches and other incidents. |
| Clock Synchronization | | | | |
| Infrastructure & Virtualization Security | Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? | | A3.2.0 | (A3.2.0) Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable. |
| Capacity / Resource Planning | | | | |
| | Do you restrict use of the memory oversubscriptioncapabilitiespresent in the hypervisor? | Yes | | (A4.1.0) The entity’s system availability andSecurityperformance is periodically reviewed and compared with the defined system availability and relatedSecuritypolicies. |
| | 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 | | |
| | 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? | | A4.1.0 | |

| | | | | |
|---|---|---|---|---|
| Infrastructure & Virtualization Security | DoSecurityvulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)? | Yes | | |
| Management - Vulnerability Management | | | | |
| Infrastructure & Virtualization Security | For your IaaS offering, do you provide customers with guidance on how to create a layeredSecurityArchitectureequivalence using your virtualized solution? | | | |
| **Network Security** | Do you regularly update networkArchitecturediagrams that include data flows betweenSecuritydomains/zones? | Yes | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| | Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) betweenSecuritydomains/zones within the network? | Yes | | |
| | Are all firewall access control lists documented with business justification? | Yes | | |

| | | | | |
|---|---|---|---|---|
| Infrastructure & Virtualization Security | 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 | | |
| OS Hardening and Base Controls | | | | |
| Infrastructure & Virtualization Security | For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | | | |
| Production / Nonproduction Environments | For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? | | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| | Do you logically and physically segregate production and non-production environments? | Yes | | |
| Infrastructure & Virtualization Security | Are system and network environments protected by a firewall or virtual firewall to ensure business and customerSecurityrequirements? | Yes | | |
| Segmentation | Are system and network environments protected by a firewall or virtual firewall to ensureCompliancewith legislative, regulatory and contractual requirements? | Yes | | |
| | | | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| | Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments? | Yes | | |
| | Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data? | Yes | | |
| Infrastructure & Virtualization Security | Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers? | | | |
| VM Security - Data Protection | Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers? | | | |

| | | | | |
|---|---|---|---|---|
| Infrastructure & Virtualization Security | Do you restrict personnel access to all hypervisor management functions or administrative consoles for systemsHostingvirtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factorAuthentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)? | Yes | | |
| VMM Security - Hypervisor Hardening | | | | |
| Infrastructure & Virtualization Security | Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic? | Yes | | |
| Wireless Security | Are policies and procedures established and mechanisms implemented to ensure wirelessSecuritysettings are enabled with strong encryption forAuthenticationand transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings) | Yes | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |
| | 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 | Do your networkArchitecturediagrams clearly identify high-risk environments and data flows that may have legalComplianceimpacts? | | S3.4 | (S3.4) Procedures exist to protect against unauthorized access to system resources. |

| | |
|---|---|
| NetworkArchitecture | 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? |
| Interoperability & Portability | Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? |
| APIs | |
| Interoperability & Portability | Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)? |
| Data Request | |
| Interoperability & Portability | 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? |
| Policy & Legal | Do you provide policies and procedures (i.e. service level agreements) governing theMigrationof application data to and from your service? |
| Interoperability & Portability | Can data import, data export and service management be conducted oversecure(e.g., non-clear text and authenticated), industry accepted standardized network protocols? |
| Standardized Network Protocols | Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved? |
| Interoperability & Portability | Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g.., OVF) to help ensure interoperability? |

|  |  |  |
|---|---|---|
| Virtualization | Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review? |  |
| Mobile Security | Do you provide anti-malware training specific to mobile devices as part of your informationSecurityawareness training? | Yes |
| Anti-Malware |  |  |
| Mobile Security | Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems? |  |
| Application Stores |  |  |

| | |
|---|---|
| Mobile Security | 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? |
| Approved Applications | |
| Mobile Security | Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices? |
| Approved Software for BYOD | |

| | | |
|---|---|---|
| Mobile Security | 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? | Yes |
| Awareness and Training | | |
| Mobile Security | Do you have a documented list of pre-approvedCloudbased services that are allowed to be used for use and storage of company business data via a mobile device? | |
| **CloudBased Services** | | |

| | |
|---|---|
| Mobile Security | Do you have a documented application validation process forTestingdevice, operating system and application compatibility issues? |
| Compatibility | |
| Mobile Security | Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage? |
| Device Eligibility | |

| | |
|---|---|
| Mobile Security<br>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)? |
| Mobile Security<br>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? |

| | | |
|---|---|---|
| Mobile Security | 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? | Yes |
| Encryption | | |
| Mobile Security | Does your mobile device policy prohibit the circumvention of built-inSecuritycontrols on mobile devices (e.g., jailbreaking or rooting)? | Yes |
| 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-inSecuritycontrols? | Yes |
| Mobile Security | Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds? | Yes |
| Legal | Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-inSecuritycontrols? | Yes |
| Mobile Security | Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices? | Yes |
| Lockout Screen | | |

|  |  |  |
|---|---|---|
| Mobile Security | Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes? |  |
| Operating Systems |  |  |
| Mobile Security | Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices? | Yes |
| Passwords | Are your password policies enforced through technical controls (i.e.MDM)? | Yes |
|  | Do your password policies prohibit the changing ofAuthenticationrequirements (i.e. password/PIN length) via a mobile device? | Yes |
| Mobile Security | Do you have a policy that requires BYOD users to perform backups of specified corporate data? |  |
| Policy | Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores? |  |
|  | Do you have a policy that requires BYOD users to use anti-malware software (where supported)? | Yes |
| Mobile Security | Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices? | Yes |
| Remote Wipe | Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices? | Yes |
| Mobile Security | Do your mobile devices have the latest available security-related patches installed upon generalReleaseby the device manufacturer or carrier? |  |
| **SecurityPatches** | Do your mobile devices allow for remote validation to download the latestSecuritypatches by company IT personnel? |  |
| Mobile Security | Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device? |  |
| Users | Does your BYOD policy specify the userRolesthat are allowed access via a BYOD-enabled device? |  |

| | | | | |
|---|---|---|---|---|
| SecurityIncident Management, E-Discovery &CloudForensics | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | Yes | | |
| Contact / Authority Maintenance | | | | |
| SecurityIncident Management, E-Discovery &CloudForensics | | | IS3.7.0 | (IS3.7.0) Procedures exist to identify, report, and act upon systemSecuritybreaches and other incidents. |
| | Do you have a documentedSecurityincident response plan? | Yes | | |
| Incident Management | | | | |
| | Do youIntegratecustomized tenant requirements into yourSecurityincident response plans? | Yes | | (S3.9.0) Procedures exist to provide that issues of noncompliance with system availability, confidentiality of data, processing integrity and relatedSecuritypolicies are promptly addressed and that corrective measures are taken on a timely basis. |
| | Do you publish aRolesand responsibilities document specifying what you vs. your tenants are responsible for duringSecurityincidents? | Yes | | |
| | Have you tested yourSecurityincident response plans in the last year? | Yes | S3.9.0 | |
| SecurityIncident Management, E-Discovery &CloudForensics | | | A2.3.0 | (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 relatedSecuritypolicies and changes andUpdatesto those policies are communicated to entity personnel responsible for implementing them. |
| | Does yourSecurityinformation and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? | Yes | | |
| **IncidentReporting** | | | C2.3.0 | |
| | | | I2.3.0 | (S2.4) The process for informing the entity about breaches of the systemSecurityand for submitting complaints is communicated to authorized users. |
| | | | S2.3.0 | |

| | | | | |
|---|---|---|---|---|
| | | | | (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 relatedSecuritypolicies and that the third party is inCompliancewith its policies. |
| | | | S2.4 | |
| | Does your logging and monitoring framework allow isolation of an incident to specific tenants? | Yes | C3.6.0 | |
| SecurityIncident Management, E-Discovery &CloudForensics | | | S2.4.0 | (S2.4.0) The process for informing the entity about system availability issues, confidentiality issues, processing integrity issues,Securityissues and breaches of the systemSecurityand for submitting complaints is communicated to authorized users. |
| Incident Response Legal Preparation | Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls? | Yes | | |
| | | | | (C3.15.0) Procedures exist to provide that issues of noncompliance with defined confidentiality and relatedSecuritypolicies are promptly addressed and that corrective measures are taken on a timely basis. |
| | Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? | Yes | | |
| | 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? | Yes | | |
| | Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? | Yes | C3.15.0 | |

| | | | | |
|---|---|---|---|---|
| SecurityIncident Management, E-Discovery &CloudForensics | | | S3.9.0 | (S3.9.0) Procedures exist to provide that issues of noncompliance withSecuritypolicies are promptly addressed and that corrective measures are taken on a timely basis. |
| Incident Response Metrics | Do you monitor and quantify the types, volumes and impacts on all informationSecurityincidents? | Yes | | |
| | | | | (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. |
| | Will you share statistical information forSecurityincident data with your tenants upon request? | | C4.1.0 | |
| Supply Chain Management, Transparency and Accountability | Do you inspect and account for data quality errors and associated risks, and work with yourCloudsupply-chain partners to correct them? | | | |
| Data Quality and Integrity | Do you design and implement controls to mitigate and contain dataSecurityrisks 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 | Do you makeSecurityincident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? | Yes | | |

**IncidentReporting**

| | | | | |
|---|---|---|---|---|
| Supply Chain Management, Transparency and Accountability | Do you collect capacity and use data for all relevant components of yourCloudservice offering? | Yes | C2.2.0 | (C2.2.0) The system security, availability, system integrity, and confidentiality and relatedSecurityobligations of users and the entity’s system security, availability, system integrity, and confidentiality and relatedSecuritycommitments to users are communicated to authorized users. |
| Network / Infrastructure Services | Do you provide tenants with capacity planning and use reports? | | | |
| Supply Chain Management, Transparency and Accountability | Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics? | Yes | | |
| Provider Internal Assessments | | | | |

| | | | | |
|---|---|---|---|---|
| Supply Chain Management, Transparency and Accountability | | | S2.2.0 | (S2.2.0) The availability, confidentiality of data, processing integrity, systemSecurityand relatedSecurityobligations of users and the entity's availability and relatedSecuritycommitments to users are communicated to authorized users. |
| Third Party Agreements | | | | |
| | | | | (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. |
| | Do you select and monitor outsourced providers inCompliancewith laws in the country where the data is processed, stored and transmitted? | | | |
| | | | | (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 relatedSecuritypolicies and that the third party is inCompliancewith its policies. |
| | | | A3.6.0 | |
| | Do you select and monitor outsourced providers inCompliancewith laws in the country where the data originates? | | | |
| | Does legal counsel review all third-party agreements? | Yes | | |
| | Do third-party agreements include provision for theSecurityand protection of information and assets? | Yes | | |
| | Do you provide the client with a list and copies of all subprocessing agreements and keep this updated? | Yes | C3.6.0 | |

| | | | | |
|---|---|---|---|---|
| Supply Chain Management, Transparency and Accountability | 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 | | |
| Supply Chain Governance Reviews | | | | |
| Supply Chain Management, Transparency and Accountability | 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 | | |
| 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)? | Yes | | |
| | Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships? | | | |
| | Do you review all agreements, policies and processes at least annually? | Yes | | |
| Supply Chain Management, Transparency and Accountability | Do you assure reasonable informationSecurityacross your information supply chain by performing an annual review? | Yes | | |
| Third Party Assessment | Does your annual review include all partners/third-party providers upon which your information supply chain depends? | Yes | | |
| Supply Chain Management, Transparency and Accountability | | | S3.1.0 | (S3.1.0) Procedures exist to (1) identify potential threats of disruption to systems operation that would impair systemSecuritycommitments and (2) assess the risks associated with the identified threats. |
| Third Party Audits | | | | |
| | Do you permit tenants to perform independent vulnerability assessments? | Yes | | |
| | | | | (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. |
| | Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks? | yes | x3.1.0 | |

| | | | | |
|---|---|---|---|---|
| Threat and Vulnerability Management<br>Antivirus / Malicious Software | Do you have anti-malware programs that support or connect to yourCloudservice 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. |
| | Do you ensure thatSecuritythreat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames? | Yes | | |
| Threat and Vulnerability Management<br>Vulnerability / Patch Management | 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 systemSecuritypolicies to enable authorized access and to prevent unauthorized access. |
| | Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? | Yes | | |
| | Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? | Yes | | |
| | Will you make the results of vulnerability scans available to tenants at their request? | | | |
| | Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems? | Yes | | |
| | Will you provide your risk-based systems patching time frames to your tenants upon request? | Yes | | |
| Threat and Vulnerability Management<br>Mobile Code | | | S3.4.0 | (S3.4.0) Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software. |
| | 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 definedSecuritypolicy? | Yes | | (S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined systemSecuritypolicies to enable authorized access and to prevent unauthorized access. |
| | Is all unauthorized mobile code prevented from executing? | Yes | S3.10.0 | |