CAIQv3.1

## CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.1

| Control Domain | Control ID | Question ID | 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 (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)? | | x | | |
| | | 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 | |
| | | 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* | 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 | | | |
| | | 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. | Does your data management policies and procedures require audits to verify data input and output integrity routines? | x | | | |
| | | AIS-03.2 | | Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? | x | | | |
| **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 | | |
| **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 develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls? | | x | | |
| | | AAC-01.2 | | Does your audit program take into account effectiveness of implementation of security operations? | | x | | |
| **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 | | | We are in pre-assessment for ISO 27001 |
| | | AAC-02.2 | | Do you conduct network penetration tests of your cloud service infrastructure at least annually? | 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 at least annually? | x | | | |
| | | AAC-02.5 | | Do you conduct independent audits at least annually? | 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 | | | |
| **Audit Assurance &** | AAC-03 | AAC-03.1 | Organizations shall create and maintain a control framework which | 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 | x | | | |
| **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:<br>• Defined purpose and scope, aligned with relevant dependencies<br>• Accessible to and understood by those who will use them<br>• Owned by a named person(s) who is responsible for their review, update, and approval<br>• Defined lines of communication, roles, and responsibilities<br>• Detailed recovery procedures, manual work-around, and reference information<br>• Method for plan invocation | Does your organization have a plan or framework for business continuity management or disaster recovery management? | x | | | |
| | | BCR-01.2 | | Do you have more than one provider for each service you depend on? | x | | | |
| | | BCR-01.3 | | Do you provide a disaster recovery capability? | x | | | |
| | | BCR-01.4 | | Do you monitor service continuity with upstream providers in the event of provider failure? | x | | | |
| | | BCR-01.5 | | Do you provide access to operational redundancy reports, including the services you rely on? | x | | | |
| | | BCR-01.6 | | Do you provide a tenant-triggered failover option? | x | | | |
| | | BCR-01.7 | | Do you share your business continuity and redundancy plans with your tenants? | x | | | |
| **Business Continuity** | BCR-02 | BCR-02.1 | Business continuity and security incident response plans shall be subject | Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to | x | | | |
| **Business Continuity** | BCR-03 | BCR-03.1 | Data center utilities services and environmental conditions (e.g., water, | Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Management & Operational Resilience** *Power / Telecommunications* | | BCR-03.2 | 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. | Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions? | x | | | |
| Business Continuity | BCR-04 | BCR-04.1 | Information system documentation (e.g., administrator and user guides, | personnel to ensure configuration, installation and operation of the information system? | x | | | |
| **Business Continuity** | BCR-05 | BCR-05.1 | Physical protection against damage from natural causes and disasters, as | Is physical damage anticipated and are countermeasures included in the design of physical protections? | x | | | |
| **Business Continuity** | BCR-06 | BCR-06.1 | To reduce the risks from environmental threats, hazards, and | 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** | BCR-07 | BCR-07.1 | Policies and procedures shall be established, and supporting business | Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance? | | | x | Not all of these are provided |
| **Management &** | | BCR-07.2 | processes and technical measures implemented, for equipment | Do you have an equipment and datacenter maintenance routine or plan? | x | | | |
| **Business Continuity** | BCR-08 | BCR-08.1 | Protection measures shall be put into place to react to natural and man- | Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? | x | | | |
| **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:<br>• Identify critical products and services<br>• Identify all dependencies, including processes, applications, business partners, and third party service providers<br>• Understand threats to critical products and services | Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ? | x | | | |
| | | BCR-09.2 | • Determine impacts resulting from planned or unplanned disruptions and how these vary over time<br>• Establish the maximum tolerable period for disruption<br>• Establish priorities for recovery<br>• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption<br>• Estimate the resources required for resumption | Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service? | x | | | |
| **Business Continuity** | BCR-10 | BCR-10.1 | Policies and procedures shall be established, and supporting business | Are policies and procedures established and made available for all personnel to adequately support services operations' roles? | x | | | |
| **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 capabilities to enforce tenant data retention policies? | x | | | |
| | | BCR-11.2 | | Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements? | x | | | |
| | | BCR-11.3 | | Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements? | x | | | |
| | | BCR-11.4 | | If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities? | x | | | |
| | | BCR-11.5 | | If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration? | x | | | |
| | | BCR-11.6 | | Does your cloud solution include software/provider independent restore and recovery capabilities? | x | | | |
| | | BCR-11.7 | | Do you test your backup or redundancy mechanisms at least annually? | x | | | |
| **Change Control &** | CCC-01 | CCC-01.1 | Policies and procedures shall be established, and supporting business | Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities? | x | | | |
| **Change Control & Configuration** | CCC-02 | CCC-02.1 | External business partners shall adhere to the same policies and | Are policies and procedures for change management, release, and testing adequately communicated to external business partners? | x | | | |
| | | CCC-02.2 | procedures for change management, release, and testing as internal | Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements? | 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 have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity? | | x | | |
| | | CCC-03.2 | | Is documentation describing known issues with certain products/services available? | x | | | |
| | | 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 | | | |
| | | CCC-03.4 | | Do you have controls in place to ensure that standards of quality are being met for all software development? | x | | | |
| | | CCC-03.5 | | Do you have controls in place to detect source code security defects for any outsourced software development activities? | x | | | |
| | | CCC-03.6 | | Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions? | x | | | |
| **Change Control &** | CCC-04 | CCC-04.1 | Policies and procedures shall be established, and supporting business | Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | x | | | |
| **Change Control & Configuration Management** | CCC-05 | CCC-05.1 | Policies and procedures shall be established for managing the risks associated with applying changes to:<br>• Business-critical or customer (tenant)-impacting (physical and virtual) | Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it? | | x | | |
| | | CCC-05.2 | | Do you have policies and procedures established for managing risks with respect to change management in production environments? | | x | | |
| | | CCC-05.3 | | Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with policy (e.g., ITIL)? | | x | | |
| **Data Security & Information Lifecycle** | DSI-01 | DSI-01.1 | Data and objects containing data shall be assigned a classification by the | Do you provide a capability to identify data and 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 | | | |
| | | DSI-01.2 | data owner based on data type, value, sensitivity, and criticality to the | Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)? | x | | | |
| **Data Security & Information Lifecycle** | DSI-02 | DSI-02.1 | Policies and procedures shall be established, and supporting business | 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 | | | |
| | | DSI-02.2 | processes and technical measures implemented, to inventory, document, | Can you ensure that data does not migrate beyond a defined geographical residency? | x | | | |
| **Data Security & Information** | DSI-03 | DSI-03.1 | Data related to electronic commerce (e-commerce) that traverses public | Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to | x | | | |
| | | DSI-03.2 | networks shall be appropriately classified and protected from fraudulent | 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, federated authentication)? | | x | | |
| **Data Security & Information Lifecycle Management** | DSI-04 | DSI-04.1 | Policies and procedures shall be established for labeling, handling, and | Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data? | x | | | |
| | | DSI-04.2 | the security of data and objects which contain data. Mechanisms for label | Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | | x | | |
| | | DSI-04.3 | inheritance shall be implemented for objects that act as aggregate | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? | | x | | |
| **Data Security &** | DSI-05 | DSI-05.1 | Production data shall not be replicated or used in non-production | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | x | | | |
| **Data Security &** | DSI-06 | DSI-06.1 | All data shall be designated with stewardship, with assigned | Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated? | x | | | |
| **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 the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data? | x | | | |
| | | 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 | | | |
| **Datacenter Security** *Asset Management* | DCS-01 | DCS-01.1 | Assets must be classified in terms of business criticality, service-level | Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements? | x | | | |
| | | DCS-01.2 | expectations, and operational continuity requirements. A complete | Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership? | x | | | |
| **Datacenter Security** | DCS-02 | DCS-02.1 | Physical security perimeters (e.g., fences, walls, barriers, guards, gates, | Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Datacenter Security** *Equipment* | DCS-03 | DCS-03.1 | Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to | Do you have a capability to use system geographic location as an authentication factor? | | x | | |
| | | DCS-03.2 | | Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location? | | x | | |
| **Datacenter Security** | DCS-04 | DCS-04.1 | Authorization must be obtained prior to relocation or transfer of | Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises? | x | | | |
| **Datacenter Security** | DCS-05 | DCS-05.1 | Policies and procedures shall be established for the secure disposal of | Can you provide tenants with your asset management policies and procedures? | | x | | |
| **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 | 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 | | | |
| | | 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 | | | |
| **Datacenter Security** | DCS-07 | DCS-07.1 | Ingress and egress to secure areas shall be constrained and monitored by | Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points? | | x | | |
| **Datacenter Security** | DCS-08 | DCS-08.1 | Ingress and egress points such as service areas and other points where | 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 | | | |
| **Datacenter Security** | DCS-09 | DCS-09.1 | Physical access to information assets and functions by users and support | Do you restrict physical access to information assets and functions by users and support personnel? | x | | | |
| **Encryption & Key** | EKM-01 | EKM-01.1 | Keys must have identifiable owners (binding keys to identities) and there | Do you have key management policies binding keys to identifiable owners? | x | | | |
| **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 | Do you have a capability to allow creation of unique encryption keys per tenant? | x | | | |
| | | 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, | Do you encrypt tenant data at rest (on disk/storage) within your environment? | x | | | |
| | | 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 have documentation establishing and defining your encryption management policies, procedures, and guidelines? | x | | | |
| **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. | Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms? | x | | | |
| | | EKM-04.2 | | Are your encryption keys maintained by the cloud consumer or a trusted key management provider? | x | | | |
| | | 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 | Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)? | x | | | |
| | | GRM-01.2 | | Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? | x | | | |
| **Governance and Risk Management** | GRM-02 | GRM-02.1 | Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: | Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification? | x | | | |
| | | GRM-02.2 | | Do you conduct risk assessments associated with data governance requirements at least once a year? | x | | | |
| **Governance and Risk** | GRM-03 | GRM-03.1 | Managers are responsible for maintaining awareness of, and complying | 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 | x | | | |
| **Governance and Risk Management** | GRM-04 | GRM-04.1 | An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes | Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? | | x | | |
| | | GRM-04.2 | | Do you review your Information Security Management Program (ISMP) at least once a year? | x | | | |
| **Governance and Risk** | GRM-05 | GRM-05.1 | Executive and line management shall take formal action to support | Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned? | | 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 | Are information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and owned 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 | | x | | |
| | | GRM-06.2 | | Are information security policies 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 | x | | | |
| | | GRM-06.3 | | Do you have agreements to ensure your providers adhere to your information security and privacy policies? | x | | | |
| | | GRM-06.4 | | Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards? | | x | | |
| | | GRM-06.5 | | Do you disclose which controls, standards, certifications, and/or regulations you comply with? | x | | | |
| **Governance and Risk Management** | 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 | Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? | x | | | |
| | | 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** | GRM-08 | GRM-08.1 | Risk assessment results shall include updates to security policies, | Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective? | x | | | |
| **Governance and Risk Management** | 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 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | x | | | |
| | | GRM-09.2 | | Do you perform, at minimum, annual reviews to your privacy and security policies? | x | | | |
| **Governance and Risk Management** | 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 | 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 | | | |
| | | GRM-10.2 | | Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories? | x | | | |
| **Governance and Risk Management** | 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 | Do you have a documented, organization-wide program in place to manage risk? | x | | | |
| | | 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 | Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets? | x | | | |
| | | HRS-01.2 | | Do you have asset return procedures outlining how assets should be returned within an established period? | x | | | |
| **Human Resources** | HRS-02 | HRS-02.1 | Pursuant to local laws, regulations, ethics, and contractual constraints, all | Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification? | x | | | |
| **Human Resources** *Employment* | HRS-03 | HRS-03.1 | Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies | Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies? | x | | | |
| | | HRS-03.2 | | Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets? | x | | | |
| **Human Resources** *Employment* | HRS-04 | HRS-04.1 | Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and | Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination? | x | | | |
| | | HRS-04.2 | | Do the above procedures and guidelines account for timely revocation of access and return of assets? | x | | | |
| **Human Resources** | HRS-05 | HRS-05.1 | Policies and procedures shall be established, and supporting business | Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from unauthorized 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 | | | |
| **Human Resources** | HRS-06 | HRS-06.1 | Requirements for non-disclosure or confidentiality agreements reflecting | 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 | | | |
| **Human Resources** | HRS-07 | HRS-07.1 | Roles and responsibilities of contractors, employees, and third-party | Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant? | x | | | |
| **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 | Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components? | x | | | |
| | | HRS-08.2 | | Do you define allowance and conditions for BYOD devices and its applications to access corporate resources? | 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 | | x | | |
| | | HRS-09.2 | | Do you specifically train your employees regarding their specific role and the information security controls they must fulfill? | x | | | |
| | | HRS-09.3 | | Do you document employee acknowledgment of training they have completed? | | x | | |
| | | HRS-09.4 | | Is successful and timely completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems? | x | | | |
| | | HRS-09.5 | | Are personnel trained and provided with awareness programs at least once a year? | x | | | |
| | | HRS-09.6 | | Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity? | x | | | |
| **Human Resources** | HRS-10 | HRS-10.1 | All personnel shall be made aware of their roles and responsibilities for: | Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *User Responsibility* | | HRS-10.2 | • Maintaining awareness and compliance with established policies and | Are personnel informed of their responsibilities for maintaining a safe and secure working environment? | x | | | |
| | | HRS-10.3 | procedures and applicable legal, statutory, or regulatory compliance | Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended? | x | | | |
| **Human Resources** | HRS-11 | HRS-11.1 | Policies and procedures shall be established to require that unattended | Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time? | x | | | |
| *Workspace* | | HRS-11.2 | workspaces do not have openly visible (e.g., on a desktop) sensitive | Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents? | x | | | |
| **Identity & Access Management** | IAM-01 | IAM-01.1 | Access to, and use of, audit tools that interact with the organization's | Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)? | x | | | |
| | | IAM-01.2 | information systems shall be appropriately segmented and restricted to | Do you monitor and log privileged access (e.g., administrator level) to information security management systems? | x | | | |
| **Identity & Access Management** | IAM-02 | IAM-02.1 | User access policies and procedures shall be established, and supporting | Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes? | x | | | |
| | | IAM-02.2 | business processes and technical measures implemented, for ensuring | Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in | x | | | |
| *User Access Policy* | | IAM-02.3 | appropriate identity, entitlement, and access management for all internal | do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege? | | x | | |
| | | IAM-02.4 | corporate and customer (tenant) users with access to data and | Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures? | x | | | |
| | | IAM-02.5 | organizationally-owned or managed (physical and virtual) application | Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)? | x | | | |
| | | IAM-02.6 | interfaces and infrastructure network and systems components. These | Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case | x | | | |
| | | IAM-02.7 | policies, procedures, processes, and measures must incorporate the | 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 | | |
| **Identity & Access** | IAM-03 | IAM-03.1 | User access to diagnostic and configuration ports shall be restricted to | Is user access to diagnostic and configuration ports restricted to authorized individuals and applications? | x | | | |
| **Identity & Access Management** | IAM-04 | IAM-04.1 | Policies and procedures shall be established to store and manage identity | Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access? | x | | | |
| | | IAM-04.2 | information about every person who accesses IT infrastructure and to | Do you manage and store the user identity of all personnel who have network access, including their level of access? | x | | | |
| **Identity & Access** | IAM-05 | IAM-05.1 | User access policies and procedures shall be established, and supporting | Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? | x | | | |
| **Identity & Access Management** | IAM-06 | IAM-06.1 | Access to the organization's own developed applications, program, or | 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 | | | |
| | | IAM-06.2 | object source code, or any other form of intellectual property (IP), and | 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** | IAM-07 | IAM-07.1 | The identification, assessment, and prioritization of risks posed by | Does your organization conduct third-party unauthorized access risk assessments? | x | | | |
| *Third Party Access* | | IAM-07.2 | 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 | Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropraite access? | x | | | |
| **Identity & Access Management** | IAM-08 | IAM-08.1 | Policies and procedures are established for permissible storage and | Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege? | | x | | |
| | | IAM-08.2 | access of identities used for authentication to ensure identities are only | based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication? | x | | | |
| *User Access* | | IAM-08.3 | accessible based on rules of least privilege and replication limitation only | Do you limit identities' replication only to users explicitly defined as business necessary? | x | | | |
| **Identity & Access Management** | IAM-09 | IAM-09.1 | Provisioning user access (e.g., employees, contractors, customers | 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, | x | | | |
| | | IAM-09.2 | (tenants), business partners and/or supplier relationships) to data and | Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), | | x | | |
| **Identity & Access Management** | IAM-10 | IAM-10.1 | User access shall be authorized and revalidated for entitlement | Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and | x | | | |
| | | IAM-10.2 | appropriateness, at planned intervals, by the organization's business | Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced? | | x | | |
| *User Access Reviews* | | IAM-10.3 | leadership or other accountable business role or function supported by | Do you ensure that remediation actions for access violations follow user access policies? | x | | | |
| | | IAM-10.4 | evidence to demonstrate the organization is adhering to the rule of least | Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data? | x | | | |
| **Identity & Access Management** | IAM-11 | IAM-11.1 | Timely de-provisioning (revocation or modification) of user access to data | Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employment, contract or agreement, change of employment or transfer within the organization? | x | | | |
| | | IAM-11.2 | and organizationally-owned or managed (physical and virtual) | 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** | IAM-12 | IAM-12.1 | Internal corporate or customer (tenant) user account credentials shall be | Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? | x | | | |
| | | IAM-12.2 | restricted as per the following, ensuring appropriate identity, | Do you use open standards to delegate authentication capabilities to your tenants? | | x | | |
| *User ID Credentials* | | IAM-12.3 | entitlement, and access management and in accordance with established | Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? | x | | | |
| | | IAM-12.4 | policies and procedures: | 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 | • Identity trust verification and service-to-service application (API) and | 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 | information processing interoperability (e.g., SSO and Federation) | Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access? | | x | | |
| | | IAM-12.7 | • Account credential lifecycle management from instantiation through | Do you allow tenants to use third-party identity assurance services? | x | | | |
| | | IAM-12.8 | revocation | Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement? | x | | | |
| | | IAM-12.9 | • Account credential and/or identity store minimization or re-use when | Do you allow tenants/customers to define password and account lockout policies for their accounts? | x | | | |
| | | IAM-12.10 | feasible | Do you support the ability to force password changes upon first logon? | x | | | |
| | | IAM-12.11 | • Adherence to industry acceptable and/or regulatory compliant | 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** | IAM-13 | IAM-13.1 | Utility programs capable of potentially overriding system, object, | Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored? | x | | | |
| **Infrastructure & Virtualization Security** | IVS-01 | IVS-01.1 | Higher levels of assurance are required for protection, retention, and | 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 | | |
| | | IVS-01.2 | lifecycle management of audit logs, adhering to applicable legal, | Is physical and logical user access to audit logs restricted to authorized personnel? | x | | | |
| *Audit Logging / Intrusion Detection* | | IVS-01.3 | statutory, or regulatory compliance obligations and providing unique user | Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed? | | x | | |
| | | IVS-01.4 | access accountability to detect potentially suspicious network behaviors | Are audit logs centrally stored and retained? | x | | | |
| | | IVS-01.5 | and/or file integrity anomalies, and to support forensic investigative | Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? | | x | | |
| **Infrastructure & Virtualization Security** | IVS-02 | IVS-02.1 | The provider shall ensure the integrity of all virtual machine images at all | Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)? | x | | | |
| | | IVS-02.2 | times. Any changes made to virtual machine images must be logged and | 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 | | | |
| | | IVS-02.3 | an alert raised regardless of their running state (e.g., dormant, off, or | 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 &** | IVS-03 | IVS-03.1 | A reliable and mutually agreed upon external time source shall be used to | Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference? | x | | | |
| **Infrastructure & Virtualization Security** | IVS-04 | IVS-04.1 | The availability, quality, and adequate capacity and resources shall be | 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 | | |
| | | IVS-04.2 | planned, prepared, and measured to deliver the required system | Do you restrict use of the memory oversubscription capabilities present in the hypervisor? | x | | | |
| *Capacity / Resource* | | IVS-04.3 | performance in accordance with legal, statutory, and regulatory | Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used | x | | | |
| | | IVS-04.4 | compliance obligations. Projections of future capacity requirements shall | Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide service to the tenants? | x | | | |
| **Infrastructure &** | IVS-05 | IVS-05.1 | Implementers shall ensure that the security vulnerability assessment | Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)? | | | x | |
| **Infrastructure & Virtualization Security** | IVS-06 | IVS-06.1 | Network environments and virtual instances shall be designed and | For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution? | | | x | |
| | | IVS-06.2 | configured to restrict and monitor traffic between trusted and untrusted | Do you regularly update network architecture diagrams that include data flows between security domains/zones? | x | | | |
| *Network Security* | | IVS-06.3 | connections. These configurations shall be reviewed at least annually, | Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network? | x | | | |
| | | IVS-06.4 | and supported by a documented justification for use for all allowed | Are all firewall access control lists documented with business justification? | x | | | |
| **Infrastructure &** | IVS-07 | IVS-07.1 | Each operating system shall be hardened to provide only necessary ports, | 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 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Infrastructure & Virtualization Security** | 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, | For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | x | | | |
| | | IVS-08.2 | | For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? | | | x | |
| | | IVS-08.3 | | Do you logically and physically segregate production and non-production environments? | x | | | |
| **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: | Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements? | x | | | |
| | | IVS-09.2 | | Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements? | x | | | |
| | | IVS-09.3 | | Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations? | x | | | |
| | | IVS-09.4 | | 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 | | | |
| | | IVS-09.5 | | Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data? | x | | | |
| **Infrastructure & Virtualization** | IVS-10 | IVS-10.1 | Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, | Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers? | x | | | |
| | | IVS-10.2 | | Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers? | x | | | |
| **Infrastructure &** | IVS-11 | IVS-11.1 | Access to all hypervisor management functions or administrative | Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized | x | | | |
| **Infrastructure & Virtualization 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: | Are policies and procedures established and mechanisms configured and implemented to protect the wireless network | x | | | |
| | | IVS-12.2 | | Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong | x | | | |
| | | IVS-12.3 | | Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the | x | | | |
| **Infrastructure & Virtualization** | IVS-13 | IVS-13.1 | Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. | Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance | x | | | |
| | | IVS-13.2 | | Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and | | x | | |
| **Interoperability &** | IPY-01 | IPY-01.1 | The provider shall use open and published APIs to ensure support for | Do you publish a list of all APIs available in the service and indicate which are standard and which are customized? | | | x | |
| **Interoperability &** | IPY-02 | IPY-02.1 | All structured and unstructured data shall be available to the customer | 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, | 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 | | | |
| | | IPY-03.2 | | If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider? | | x | | |
| | | IPY-03.3 | | Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your | x | | | |
| **Interoperability & Portability** | 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 | Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry | x | | | |
| | | IPY-04.2 | | Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol | 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 | Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure | x | | | |
| | | IPY-05.2 | | If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to | x | | | |
| | | IPY-05.3 | | Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for | x | | | |
| **Mobile Security** | MOS-01 | MOS-01.1 | Anti-malware awareness training, specific to mobile devices, shall be | Do you provide anti-malware training specific to mobile devices as part of your information security awareness training? | | | x | We do not provide mobile |
| **Mobile Security** | MOS-02 | MOS-02.1 | A documented list of approved application stores has been | Do you document and make available lists of approved application stores for mobile devices accessing or storing company data | | | x | |
| **Mobile Security** | MOS-03 | MOS-03.1 | The company shall have a documented policy prohibiting the installation | Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved | | | x | |
| **Mobile Security** | MOS-04 | MOS-04.1 | The BYOD policy and supporting awareness training clearly states the | Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices? | | | x | |
| **Mobile Security** | MOS-05 | MOS-05.1 | The provider shall have a documented mobile device policy that includes | Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted | x | | | |
| **Mobile Security** | MOS-06 | MOS-06.1 | All cloud-based services used by the company's mobile devices or BYOD | Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company | x | | | |
| **Mobile Security** | MOS-07 | MOS-07.1 | The company shall have a documented application validation process to | Do you have a documented application validation process for testing device, operating system, and application compatibility | | | x | |
| **Mobile Security** | MOS-08 | MOS-08.1 | The BYOD policy shall define the device and eligibility requirements to | Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage? | | | x | |
| **Mobile Security** | MOS-09 | MOS-09.1 | An inventory of all mobile devices used to store and access company data | Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., | | | x | |
| **Mobile Security** | MOS-10 | MOS-10.1 | A centralized, mobile device management solution shall be deployed to | Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, | | | x | |
| **Mobile Security** | MOS-11 | MOS-11.1 | The mobile device policy shall require the use of encryption either for the | Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive | | | x | |
| **Mobile Security** *Jailbreaking and* | 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 | Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or | | | x | |
| | | MOS-12.2 | | Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the | | | 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 | Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds? | | | x | |
| | | MOS-13.2 | | Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required? | | | x | |
| **Mobile Security** | MOS-14 | MOS-14.1 | BYOD and/or company owned devices are configured to require an | Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices? | | | x | |
| **Mobile Security** | MOS-15 | MOS-15.1 | Changes to mobile device operating systems, patch levels, and/or | Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change | | | 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 | 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 | |
| | | 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 | 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 | Do your mobile devices have the latest available security-related patches installed upon general release by the device | | | x | |
| | | 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** | SEF-01 | SEF-01.1 | Points of contact for applicable regulation authorities, national and local | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | x | | | |
| **Security Incident Management, E-Discovery, & Cloud Forensics** | 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 | | | |
| | | SEF-02.2 | | Do you integrate customized tenant requirements into your security incident response plans? | x | | | |
| | | SEF-02.3 | | Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security | 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. | Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner? | x | | | |
| | | SEF-03.2 | | Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations? | x | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Security Incident Management, E-Discovery, & Cloud Forensics** | 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 | 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-** | 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 | | | |
| **Supply Chain Management,** | 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. | Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them? | x | | | |
| | | STA-01.2 | | Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based | x | | | |
| **Supply Chain** | STA-02 | STA-02.1 | The provider shall make security incident information available to all | Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)? | x | | | |
| **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 | | | |
| | | STA-03.2 | | Do you provide tenants with capacity planning and use reports? | | x | | |
| **Supply Chain** | STA-04 | STA-04.1 | The provider shall perform annual internal assessments of conformance | Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting | x | | | |
| **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:<br>• 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)<br>• 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 | Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted? | x | | | |
| | | STA-05.2 | | Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation? | x | | | |
| | | STA-05.3 | | Does legal counsel review all third-party agreements? | x | | | |
| | | STA-05.4 | | Do third-party agreements include provision for the security and protection of information and assets? | x | | | |
| | | STA-05.5 | | Do you have the capability to recover data for a specific customer in the case of a failure or data loss? | x | | | |
| | | STA-05.6 | | Do you have the capability to restrict the storage of customer data to specific countries or geographic locations? | x | | | |
| | | STA-05.7 | | Can you provide the physical location/geography of storage of a tenant's data upon request? | x | | | |
| | | STA-05.8 | | Can you provide the physical location/geography of storage of a tenant's data in advance? | x | | | |
| | | STA-05.9 | | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | x | | | |
| | | STA-05.10 | | Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data? | | x | | |
| | | STA-05.11 | | Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies? | x | | | |
| | | STA-05.12 | | Do you provide the client with a list and copies of all subprocessing agreements and keep this updated? | x | | | |
| **Supply Chain** | STA-06 | STA-06.1 | Providers shall review the risk management and governance processes of | Do you review the risk management and governance processes of partners to account for risks inherited from other members of the partner's supply chain? | x | | | |
| **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 | 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 provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance? | x | | | |
| | | STA-07.5 | | Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants? | x | | | |
| | | STA-07.6 | | Do you provide customers with ongoing visibility and reporting of your SLA performance? | | x | | |
| | | STA-07.7 | | Do your data management policies and procedures address tenant and service level conflicts of interests? | | x | | |
| | | STA-07.8 | | Do you review all service level agreements at least annually? | x | | | |
| **Supply Chain Management,** | STA-08 | STA-08.1 | Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review | Do you assure reasonable information security across your information supply chain by performing an annual review? | x | | | |
| | | STA-08.2 | | Does your annual review include all partners/third-party providers upon which your information supply chain depends? | x | | | |
| **Supply Chain Management,** | STA-09 | STA-09.1 | Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service | Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met? | | x | | |
| | | STA-09.2 | | Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and | x | | | |
| **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 IT infrastructure network and systems components? | x | | | |
| | | TVM-01.2 | | Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices? | | x | | |
| **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 | Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? | x | | | |
| | | TVM-02.2 | | Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? | x | | | |
| | | TVM-02.3 | | Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? | x | | | |
| | | TVM-02.4 | | Will you make the results of vulnerability scans available to tenants at their request? | x | | | |
| | | TVM-02.5 | | Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems? | x | | | |
| | | TVM-02.6 | | Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control? | x | | | |
| **Threat and** | TVM-03 | TVM-03.1 | Policies and procedures shall be established, and supporting business | 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 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Vulnerability Management** *Mobile Code* | | TVM-03.2 | 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 | Is all unauthorized mobile code prevented from executing? | x | | | |