

Cloud Security Alliance (CAIQ) Questionnaire

1. Contact Information

1.1 Third-Party Provider Name*

1.2 Location of Data Center*

1.3 Address*

1.4 Location of Recovery Center

1.5 IT Security Contact

1.6 Phone*

1.7 E-mail*

1.8 Web site*

1.9 Description of Service/Product (include technical details, e.g. client, agent, SSL, FTP transmission, hosted website, ASP, etc.)*

1.10 Describe Pertinent Outsourced/Contracted Service Arrangements (e.g. onsite support, remote support, temporary access, database management, etc.)*

2. A&A Audit & Assurance

A&A-01 Audit and Assurance Policy and Procedures

- 2.1 A&A-01.1 Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?*
- 2.2 A&A-01.2 Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?*

A&A-02 Independent Assessments

- 2.3 A&A-02.1 Are independent audit and assurance assessments conducted according to relevant standards at least annually?*

A&A-03 Risk Based Planning Assessment

- 2.4 A&A-03.1 Are independent audit and assurance assessments performed according to risk-based plans and policies?*

A&A-04 Requirements Compliance

- 2.5 A&A-04.1 Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?*

A&A-05 Audit Management Process

- 2.6 A&A-05.1 Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?*

A&A-06 Remediation

- 2.7 A&A-06.1 Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?*
- 2.8 A&A-06.2 Is the remediation status of audit findings reviewed and reported to relevant stakeholders?*

3. AIS Application & Interface Security

AIS-01 Application and Interface Security Policy and Procedures

3.1 AIS-01.1 Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?*

3.2 AIS-01.2 Are application security policies and procedures reviewed and updated at least annually?*

AIS-02 Application Security Baseline Requirements

3.3 AIS-02.1 Are baseline requirements to secure different applications established, documented, and maintained?*

AIS-03 Application Security Metrics

3.4 AIS-03.1 Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?*

AIS-04 Secure Application Design and Development

3.5 AIS-04.1 Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?*

AIS-05 Automated Application Security Testing

3.6 AIS-05.1 Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?*

3.7 AIS-05.2 Is testing automated when applicable and possible?*

AIS-06 Automated Secure Application Deployment

3.8 AIS-06.1 Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?*

3.9 AIS-06.2 Is the deployment and integration of application code automated where possible?*

AIS-07 Application Vulnerability Remediation

3.10 AIS-07.1 Are application security vulnerabilities remediated following defined processes?*

3.11 AIS-07.2 Is the remediation of application security vulnerabilities automated when possible?*

4. BCR Business Continuity Management and Operational Resilience

BCR-01 Business Continuity Management Policy and Procedures

4.1 BCR-01.1 Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?*

4.2 BCR-01.2 Are the policies and procedures reviewed and updated at least annually?*

BCR-02 Risk Assessment and Impact Analysis

4.3 BCR-02.1 Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?*

BCR-03 Business Continuity Strategy

4.4 BCR-03.1 Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?*

BCR-04 Business Continuity Planning

4.5 BCR-04.1 Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?*

BCR-05 Documentation

4.6 BCR-05.1 Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?*

4.7 BCR-05.2 Is business continuity and operational resilience documentation available to authorized stakeholders?*

4.8 BCR-05.3 Is business continuity and operational resilience documentation reviewed periodically?*

BCR-06 Business Continuity Exercises

4.9 BCR-06.1 Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?*

BCR-07 Communication

4.10 BCR-07.1 Do business continuity and resilience procedures establish communication with stakeholders and participants?*

BCR-08 Backup

4.11 BCR-08.1 Is cloud data periodically backed up?*

4.12 BCR-08.2 Is the confidentiality, integrity, and availability of backup data ensured?*

4.13 BCR-08.3 Can backups be restored appropriately for resiliency?*

BCR-09 Disaster Response Plan

4.14 BCR-09.1 Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?*

4.15 BCR-09.2 Is the disaster response plan updated at least annually, and when significant changes occur?*

BCR-10 Response Plan Exercise

4.16 BCR-10.1 Is the disaster response plan exercised annually or when significant changes occur?*

4.17 BCR-10.2 Are local emergency authorities included, if possible, in the exercise?*

BCR-11 Equipment Redundancy

4.18 BCR-11.1 Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?*

5. CCC Change Control and Configuration Management

CCC-01 Change Management Policy and Procedures

5.1 CCC-01.1 Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?*

5.2 CCC-01.2 Are the policies and procedures reviewed and updated at least annually?*

CCC-02 Quality Testing

5.3 CCC-02.1 Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?*

CCC-03 Change Management Technology

5.4 CCC-03.1 Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?*

CCC-04 Unauthorized Change Protection

5.5 CCC-04.1 Is the unauthorized addition, removal, update, and management of organization assets restricted?*

CCC-05 Change Agreements

5.6 CCC-05.1 Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?*

CCC-06 Change Management Baseline

5.7 CCC-06.1 Are change management baselines established for all relevant authorized changes on organizational assets?*

CCC-07 Detection of Baseline Deviation

5.8 CCC-07.1 Are detection measures implemented with proactive notification if changes deviate from established baselines?*

CCC-08 Exception Management

5.9 CCC-08.1 Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?*

5.10 CCC-08.2 Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?*

CCC-09 Change Restoration

5.11 CCC-09.1 Is a process to proactively roll back changes to a previously known 'good state' defined and implemented in case of errors or security concerns?*

6. CEK Cryptography, Encryption & Key Management

CEK-01 Encryption and Key Management Policy and Procedures

6.1 CEK-01.1 Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?*

6.2 CEK-01.2 Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?*

CEK-02 CEK Roles and Responsibilities

6.3 CEK-02.1 Are cryptography, encryption, and key management roles and responsibilities defined and implemented?*

CEK-03 Data Encryption

6.4 CEK-03.1 Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?*

CEK-04 Encryption Algorithm

6.5 CEK-04.1 Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?*

CEK-05 Encryption Change Management

6.6 CEK-05.1 Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?*

CEK-06 Encryption Change Cost Benefit Analysis

6.7 CEK-06.1 Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?*

CEK-07 Encryption Risk Management

6.8 CEK-07.1 Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?*

CEK-08 CSC Key Management Capability

6.9 CEK-08.1 Are CSPs providing CSCs with the capacity to manage their own data encryption keys?*

CEK-09 Encryption and Key Management Audit

6.10 CEK-09.1 Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?*

6.11 CEK-09.2 Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?*

CEK-10 Key Generation

6.12 CEK-10.1 Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?*

CEK-11 Key Purpose

6.13 CEK-11.1 Are private keys provisioned for a unique purpose managed, and is cryptography secret?*

CEK-12 Key Rotation

6.14 CEK-12.1 Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?*

CEK-13 Key Revocation

6.15 CEK-13.1 Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?*

CEK-14 Key Destruction

6.16 CEK-14.1 Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?*

CEK-15 Key Activation

6.17 CEK-15.1 Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-16 Key Suspension

6.18 CEK-16.1 Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-17 Key Deactivation

6.19 CEK-17.1 Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-18 Key Archival

6.20 CEK-18.1 Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-19 Key Compromise

6.21 CEK-19.1 Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-20 Key Recovery

6.22 CEK-20.1 Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?*

CEK-21 Key Inventory Management

6.23 CEK-21.1 Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?*

7. DCS Datacenter Security

DCS-01 Off-Site Equipment Disposal Policy and Procedures

- 7.1 DCS-01.1 Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?*
- 7.2 DCS-01.2 Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?*
- 7.3 DCS-01.3 Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?*

DCS-02 Off-Site Transfer Authorization Policy and Procedures

- 7.4 DCS-02.1 Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?*
- 7.5 DCS-02.2 Does a relocation or transfer request require written or cryptographically verifiable authorization?*
- 7.6 DCS-02.3 Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?*

DCS-03 Secure Area Policy and Procedures

- 7.7 DCS-03.1 Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?*
- 7.8 DCS-03.2 Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?*

DCS-04 Secure Media Transportation Policy and Procedures

- 7.9 DCS-04.1 Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?*

7.10 DCS-04.2 Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?*

DCS-05 Assets Classification

7.11 DCS-05.1 Is the classification and documentation of physical and logical assets based on the organizational business risk?*

DCS-06 Assets Cataloguing and Tracking

7.12 DCS-06.1 Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?*

DCS-07 Controlled Access Points

7.13 DCS-07.1 Are physical security perimeters implemented to safeguard personnel, data, and information systems?*

7.14 DCS-07.2 Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?*

DCS-08 Equipment Identification

7.15 DCS-08.1 Is equipment identification used as a method for connection authentication?*

DCS-09 Secure Area Authorization

7.16 DCS-09.1 Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?*

7.17 DCS-09.2 Are access control records retained periodically, as deemed appropriate by the organization?*

DCS-10 Surveillance System

7.18 DCS-10.1 Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?*

DCS-11 Unauthorized Access Response Training

7.19 DCS-11.1 Are datacenter personnel trained to respond to unauthorized access or egress attempts?*

DCS-12 Cabling Security

7.20 DCS-12.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?*

DCS-13 Environmental Systems

7.21 DCS-13.1 Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?*

DCS-14 Secure Utilities

7.22 DCS-14.1 Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?*

DCS-15 Equipment Location

7.23 DCS-15.1 Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?*

8. DSP Data Security and Privacy Lifecycle Management

DSP-01 Security and Privacy Policy and Procedures

8.1 DSP-01.1 Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?*

8.2 DSP-01.2 Are data security and privacy policies and procedures reviewed and updated at least annually?*

DSP-02 Secure Disposal

8.3 DSP-02.1 Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?*

DSP-03 Data Inventory

8.4 DSP-03.1 Is a data inventory created and maintained for sensitive and personal information (at a minimum)?*

DSP-04 Data Classification

8.5 DSP-04.1 Is data classified according to type and sensitivity levels?*

DSP-05 Data Flow Documentation

8.6 DSP-05.1 Is data flow documentation created to identify what data is processed and where it is stored and transmitted?*

8.7 DSP-05.2 Is data flow documentation reviewed at defined intervals, at least annually, and after any change?*

DSP-06 Data Ownership and Stewardship

8.8 DSP-06.1 Is the ownership and stewardship of all relevant personal and sensitive data documented?*

8.9 DSP-06.2 Is data ownership and stewardship documentation reviewed at least annually?*

DSP-07 Data Protection by Design and Default

8.10 DSP-07.1 Are systems, products, and business practices based on security principles by design and per industry best practices?*

DSP-08 Data Privacy by Design and Default

8.11 DSP-08.1 Are systems, products, and business practices based on privacy principles by design and according to industry best practices?*

8.12 DSP-08.2 Are systems' privacy settings configured by default and according to all applicable laws and regulations?*

DSP-09 Data Protection Impact Assessment

8.13 DSP-09.1 Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?*

DSP-10 Sensitive Data Transfer

8.14 DSP-10.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?*

DSP-11 Personal Data Access, Reversal, Rectification and Deletion

8.15 DSP-11.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?*

DSP-12 Limitation of Purpose in Personal Data Processing

8.16 DSP-12.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?*

DSP-13 Personal Data Sub-processing

8.17 DSP-13.1 Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?*

DSP-14 Disclosure of Data Sub-processors

8.18 DSP-14.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation)?*

DSP-15 Limitation of Production Data Use

8.19 DSP-15.1 Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments)?*

DSP-16 Data Retention and Deletion

8.20 DSP-16.1 Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations)?*

DSP-17 Sensitive Data Protection

8.21 DSP-17.1 Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle)?*

DSP-18 Disclosure Notification

8.22 DSP-18.1 Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations)?*

8.23 DSP-18.2 Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?*

DSP-19 Data Location

8.24 DSP-19.1 Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?*

9. GRC Governance, Risk and Compliance

GRC-01 Governance Program Policy and Procedures

9.1 GRC-01.1 Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?*

9.2 GRC-01.2 Are the policies and procedures reviewed and updated at least annually?*

GRC-02 Risk Management Program

9.3 GRC-02.1 Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?*

GRC-03 Organizational Policy Reviews

9.4 GRC-03.1 Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?*

GRC-04 Policy Exception Process

9.5 GRC-04.1 Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?*

GRC-05 Information Security Program

9.6 GRC-05.1 Has an information security program (including programs of all relevant CCM domains) been developed and implemented?*

GRC-06 Governance Responsibility Model

9.7 GRC-06.1 Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?*

GRC-07 Information System Regulatory Mapping

9.8 GRC-07.1 Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?*

GRC-08 Special Interest Groups

9.9 GRC-08.1 Is contact established and maintained with cloud-related special interest groups and other relevant entities?*

10. HRS Human Resources

HRS-01 Background Screening Policy and Procedures

- 10.1 HRS-01.1 Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?*
- 10.2 HRS-01.2 Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?*
- 10.3 HRS-01.3 Are background verification policies and procedures reviewed and updated at least annually?*

HRS-02 Acceptable Use of Technology Policy and Procedures

- 10.4 HRS-02.1 Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?*
- 10.5 HRS-02.2 Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?*

HRS-03 Clean Desk Policy and Procedures

- 10.6 HRS-03.1 Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?*
- 10.7 HRS-03.2 Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?*

HRS-04 Remote and Home Working Policy and Procedures

- 10.8 HRS-04.1 Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?*

10.9 HRS-04.2 Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?*

HRS-05 Asset returns

10.10 HRS-05.1 Are return procedures of organizationally-owned assets by terminated employees established and documented?*

HRS-06 Employment Termination

10.11 HRS-06.1 Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?*

HRS-07 Employment Agreement Process

10.12 HRS-07.1 Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?*

HRS-08 Employment Agreement Content

10.13 HRS-08.1 Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?*

HRS-09 Personnel Roles and Responsibilities

10.14 HRS-09.1 Are employee roles and responsibilities relating to information assets and security documented and communicated?*

HRS-10 Non-Disclosure Agreements

10.15 HRS-10.1 Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?*

HRS-11 Security Awareness Training

10.16 HRS-11.1 Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?*

10.17 HRS-11.2 Are regular security awareness training updates provided?*

HRS-12 Personal and Sensitive Data Awareness and Training

10.18 HRS-12.1 Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?*

10.19 HRS-12.2 Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?

*

HRS-13 Compliance User Responsibility

10.20 HRS-13.1 Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?*

11. IAM Identity & Access Management

IAM-01 Identity and Access Management Policy and Procedures

11.1 IAM-01.1 Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?*

11.2 IAM-01.2 Are identity and access management policies and procedures reviewed and updated at least annually?*

IAM-02 Strong Password Policy and Procedures

11.3 IAM-02.1 Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?*

11.4 IAM-02.2 Are strong password policies and procedures reviewed and updated at least annually?*

IAM-03 Identity Inventory

11.5 IAM-03.1 Is system identity information and levels of access managed, stored, and reviewed?*

IAM-04 Separation of Duties

11.6 IAM-04.1 Is the separation of duties principle employed when implementing information system access?*

IAM-05 Least Privilege

11.7 IAM-05.1 Is the least privilege principle employed when implementing information system access?*

IAM-06 User Access Provisioning

11.8 IAM-06.1 Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?*

IAM-07 User Access Changes and Revocation

11.9 IAM-07.1 Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?*

IAM-08 User Access Review

11.10 IAM-08.1 Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?*

IAM-09 Segregation of Privileged Access Roles

11.11 IAM-09.1 Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?*

IAM-10 Management of Privileged Access Roles

11.12 IAM-10.1 Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?*

11.13 IAM-10.2 Are procedures implemented to prevent the culmination of segregated privileged access?

*

IAM-11 CSCs Approval for Agreed Privileged Access Roles

11.14 IAM-11.1 Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?*

IAM-12 Safeguard Logs Integrity

11.15 IAM-12.1 Are processes, procedures, and technical measures to ensure the logging infrastructure is 'read-only' for all with write access (including privileged access roles) defined, implemented, and evaluated?*

11.16 IAM-12.2 Is the ability to disable the 'read-only' configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?*

IAM-13 Uniquely Identifiable Users

11.17 IAM-13.1 Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?*

IAM-14 Strong Authentication

11.18 IAM-14.1 Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?*

11.19 IAM-14.2 Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?*

IAM-15 Passwords Management

11.20 IAM-15.1 Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?*

IAM-16 Authorization Mechanisms

11.21 IAM-16.1 Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?*

12. IPY Interoperability & Portability

IPY-01 Interoperability and Portability Policy and Procedures

12.1 IPY-01.1 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?*

12.2 IPY-01.2 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?*

12.3 IPY-01.3 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?*

12.4 IPY-01.4 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?*

12.5 IPY-01.5 Are interoperability and portability policies and procedures reviewed and updated at least annually?*

IPY-02 Application Interface Availability

12.6 IPY-02.1 Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?*

IPY-03 Secure Interoperability and Portability Management

12.7 IPY-03.1 Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?*

IPY-04 Data Portability Contractual Obligations

12.8 IPY-04.1 Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format, b. Duration data will be stored, c. Scope of the data retained and made available to the CSCs, d. Data deletion policy*

13. IVS Infrastructure & Virtualization Security

IVS-01 Infrastructure and Virtualization Security Policy and Procedures

13.1 IVS-01.1 Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?*

13.2 IVS-01.2 Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?*

IVS-02 Capacity and Resource Planning

13.3 IVS-02.1 Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?*

IVS-03 Network Security

13.4 IVS-03.1 Are communications between environments monitored?*

13.5 IVS-03.2 Are communications between environments encrypted?*

13.6 IVS-03.3 Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?*

13.7 IVS-03.4 Are network configurations reviewed at least annually?*

13.8 IVS-03.5 Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?*

IVS-04 OS Hardening and Base Controls

13.9 IVS-04.1 Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?*

IVS-05 Production and Non-Production Environments

13.10 IVS-05.1 Are production and non-production environments separated?*

IVS-06 Segmentation and Segregation

13.11 IVS-06.1 Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?*

IVS-07 Migration to Cloud Environments

13.12 IVS-07.1 Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?*

IVS-08 Network Architecture Documentation

13.13 IVS-08.1 Are high-risk environments identified and documented?*

IVS-09 Network Defense

13.14 IVS-09.1 Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?*

14. LOG Logging and Monitoring

LOG-01 Logging and Monitoring Policy and Procedures

14.1 LOG-01.1 Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?*

14.2 LOG-01.2 Are policies and procedures reviewed and updated at least annually?*

LOG-02 Audit Logs Protection

14.3 LOG-02.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?*

LOG-03 Security Monitoring and Alerting

14.4 LOG-03.1 Are security-related events identified and monitored within applications and the underlying infrastructure?*

14.5 LOG-03.2 Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?*

LOG-04 Audit Logs Access and Accountability

14.6 LOG-04.1 Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?*

LOG-05 Audit Logs Monitoring and Response

14.7 LOG-05.1 Are security audit logs monitored to detect activity outside of typical or expected patterns?*

14.8 LOG-05.2 Is a process established and followed to review and take appropriate and timely actions on detected anomalies?*

LOG-06 Clock Synchronization

14.9 LOG-06.1 Is a reliable time source being used across all relevant information processing systems?*

LOG-07 Logging Scope

14.10 LOG-07.1 Are logging requirements for information meta/data system events established, documented, and implemented?*

14.11 LOG-07.2 Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?*

LOG-08 Log Records

14.12 LOG-08.1 Are audit records generated, and do they contain relevant security information?*

LOG-09 Log Protection

14.13 LOG-09.1 Does the information system protect audit records from unauthorized access, modification, and deletion?*

LOG-10 Encryption Monitoring and Reporting

14.14 LOG-10.1 Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?*

LOG-11 Transaction/Activity Logging

14.15 LOG-11.1 Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?*

LOG-12 Access Control Logs

14.16 LOG-12.1 Is physical access logged and monitored using an auditable access control system?*

LOG-13 Failures and Anomalies Reporting

14.17 LOG-13.1 Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?*

14.18 LOG-13.2 Are accountable parties immediately notified about anomalies and failures?*

15. SEF Security Incident Management, E-Discovery, & Cloud Forensics

SEF-01 Security Incident Management Policy and Procedures

15.1 SEF-01.1 Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?*

15.2 SEF-01.2 Are policies and procedures reviewed and updated annually?*

SEF-02 Service Management Policy and Procedures

15.3 SEF-02.1 Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?*

15.4 SEF-02.2 Are policies and procedures for timely management of security incidents reviewed and updated at least annually?*

SEF-03 Incident Response Plans

15.5 SEF-03.1 Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?*

SEF-04 Incident Response Testing

15.6 SEF-04.1 Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?*

SEF-05 Incident Response Metrics

15.7 SEF-05.1 Are information security incident metrics established and monitored?*

SEF-06 Event Triage Processes

15.8 SEF-06.1 Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?*

SEF-07 Security Breach Notification

15.9 SEF-07.1 Are processes, procedures, and technical measures for security breach notifications defined and implemented?*

15.10 SEF-07.2 Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?*

SEF-08 Points of Contact Maintenance

15.11 SEF-08.1 Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?*

16. STA Supply Chain Management, Transparency, and Accountability

STA-01 SSRM Policy and Procedures

16.1 STA-01.1 Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?*

16.2 STA-01.2 Are the policies and procedures that apply the SSRM reviewed and updated annually?*

STA-02 SSRM Supply Chain

16.3 STA-02.1 Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?*

STA-03 SSRM Guidance

16.4 STA-03.1 Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?*

STA-04 SSRM Control Ownership

16.5 STA-04.1 Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?*

STA-05 SSRM Documentation Review

16.6 STA-05.1 Is SSRM documentation for all cloud services the organization uses reviewed and validated?*

STA-06 SSRM Control Implementation

16.7 STA-06.1 Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?*

STA-07 Supply Chain Inventory

16.8 STA-07.1 Is an inventory of all supply chain relationships developed and maintained?*

STA-08 Supply Chain Risk Management

16.9 STA-08.1 Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?*

STA-09 Primary Service and Contractual Agreement

16.10 STA-09.1 Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? a) Scope, characteristics, and location of business relationship and services offered, b) Information security requirements (including SSRM), c) Change management process, d) Logging and monitoring capability, e) Incident management and communication procedures, f) Right to audit and third-party assessment, g) Service termination, h) Interoperability and portability requirements, i) Data privacy*

STA-10 Supply Chain Agreement Review

16.11 STA-10.1 Are supply chain agreements between CSPs and CSCs reviewed at least annually?*

STA-11 Internal Compliance Testing

16.12 STA-11.1 Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?*

STA-12 Supply Chain Service Agreement Compliance

16.13 STA-12.1 Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?*

STA-13 Supply Chain Governance Review

16.14 STA-13.1 Are supply chain partner IT governance policies and procedures reviewed periodically?*

STA-14 Supply Chain Data Security Assessment

16.15 STA-14.1 Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?*

17. TVM Threat & Vulnerability Management

TVM-01 Threat and Vulnerability Management Policy and Procedures

- 17.1 TVM-01.1 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?*
- 17.2 TVM-01.2 Are threat and vulnerability management policies and procedures reviewed and updated at least annually?*

TVM-02 Malware Protection Policy and Procedures

- 17.3 TVM-02.1 Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?*
- 17.4 TVM-02.2 Are asset management and malware protection policies and procedures reviewed and updated at least annually?*

TVM-03 Vulnerability Remediation Schedule

- 17.5 TVM-03.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?*

TVM-04 Detection Updates

- 17.6 TVM-04.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?*

TVM-05 External Library Vulnerabilities

- 17.7 TVM-05.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?*

TVM-06 Penetration Testing

17.8 TVM-06.1 Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?*

TVM-07 Vulnerability Identification

17.9 TVM-07.1 Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?*

TVM-08 Vulnerability Prioritization

17.10 TVM-08.1 Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?*

TVM-09 Vulnerability Management Reporting

17.11 TVM-09.1 Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?*

TVM-10 Vulnerability Management Metrics

17.12 TVM-10.1 Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?*

18. UEM Universal Endpoint Management

UEM-01 Endpoint Devices Policy and Procedures

18.1 UEM-01.1 Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?*

18.2 UEM-01.2 Are universal endpoint management policies and procedures reviewed and updated at least annually?*

UEM-02 Application and Service Approval

18.3 UEM-02.1 Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?*

UEM-03 Compatibility

18.4 UEM-03.1 Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?*

UEM-04 Endpoint Inventory

18.5 UEM-04.1 Is an inventory of all endpoints used and maintained to store and access company data?*

UEM-05 Endpoint Management

18.6 UEM-05.1 Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?*

UEM-06 Automatic Lock Screen

18.7 UEM-06.1 Are all relevant interactive-use endpoints configured to require an automatic lock screen?*

*

UEM-07 Operating Systems

18.8 UEM-07.1 Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?*

UEM-08 Storage Encryption

18.9 UEM-08.1 Is information protected from unauthorized disclosure on managed endpoints with storage encryption?*

UEM-09 Anti-Malware Detection and Prevention

18.10 UEM-09.1 Are anti-malware detection and prevention technology services configured on managed endpoints?*

UEM-10 Software Firewall

18.11 UEM-10.1 Are software firewalls configured on managed endpoints?*

UEM-11 Data Loss Prevention

18.12 UEM-11.1 Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?*

UEM-12 Remote Locate

18.13 UEM-12.1 Are remote geolocation capabilities enabled for all managed mobile endpoints?*

UEM-13 Remote Wipe

18.14 UEM-13.1 Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?*

UEM-14 Third-Party Endpoint Security Posture

18.15 UEM-14.1 Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?*