

**CLOUD CONTROLS MATRIX VERSION 4.0**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Control Domain** | **Control Title** | **Control ID** | **Updated Control Specification** | **Note** |
|  | **Audit & Assurance - A&A** | | | |  |
|  | Audit & Assurance | Audit and Assurance Policy and Procedures | **A&A-01** | Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually. |  |
|  | Audit & Assurance | Independent Assessments | **A&A-02** | Conduct independent audit and assurance assessments according to relevant standards at least annually. |  |
|  | Audit & Assurance | Risk Based Planning Assessment | A&A-03 | Perform independent audit and assurance assessments according to risk-based plans and policies. |  |
|  | Audit & Assurance | Requirements Compliance | A&A-04 | Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. |  |
|  | Audit & Assurance | Audit Management Process | A&A-05 | Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. |  |
|  | Audit & Assurance | Remediation | A&A-06 | Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders. |  |
|  | **Application & Interface Security - AIS** | | | |  |
|  | Application & Interface Security | Application and Interface Security Policy and Procedures | **AIS-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually. |  |
|  | Application & Interface Security | Application Security Baseline Requirements | **AIS-02** | Establish, document and maintain baseline requirements for securing different applications. |  |
|  | Application & Interface Security | Application Security Metrics | **AIS-03** | Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. |  |
|  | Application & Interface Security | Secure Application Design and Development | **AIS-04** | Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. |  |
|  | Application & Interface Security | Automated Application Security Testing | **AIS-05** | Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible. |  |
|  | Application & Interface Security | Automated Secure Application Deployment | **AIS-06** | Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible. |  |
|  | Application & Interface Security | Application Vulnerability Remediation | **AIS-07** | Define and implement a process to remediate application security vulnerabilities, automating remediation when possible. |  |
|  | **Business Continuity Management and Operational Resilience - BCR** | | | |  |
|  | Business Continuity Management & Operational Resilience | Business Continuity Management Policy and Procedures | **BCR-01** | Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually. |  |
|  | Business Continuity Management & Operational Resilience | Risk Assessment and Impact Analysis | **BCR-02** | Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. |  |
|  | Business Continuity Management & Operational Resilience | Business Continuity Strategy | **BCR-03** | Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite. |  |
|  | Business Continuity Management & Operational Resilience | Business Continuity Planning | **BCR-04** | Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities. |  |
|  | Business Continuity Management & Operational Resilience | Documentation | **BCR-05** | Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically. |  |
|  | Business Continuity Management & Operational Resilience | Business Continuity Exercises | **BCR-06** | Exercise and test business continuity and operational resilience plans at least annually or upon significant changes. |  |
|  | Business Continuity Management & Operational Resilience | Communication | **BCR-07** | Establish communication with stakeholders and participants in the course of business continuity and resilience procedures. |  |
|  | Business Continuity Management & Operational Resilience | Backup | **BCR-08** | Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency. |  |
|  | Business Continuity Management & Operational Resilience | Disaster Response Plan | **BCR-09** | Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes. |  |
|  | Business Continuity Management & Operational Resilience | Response Plan Exercise | **BCR-10** | Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities. |  |
|  | Business Continuity Management & Operational Resilience | Equipment Redundancy | **BCR-11** | Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. |  |
|  | **Change Control and Configuration Management - CCC** | | | |  |
|  | Change Control & Configuration Management | Change Management Policy and Procedures | **CCC-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually. |  |
|  | Change Control & Configuration Management | Quality Testing | **CCC-02** | Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards. |  |
|  | Change Control & Configuration Management | Change Management Technology | **CCC-03** | Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). |  |
|  | Change Control & Configuration Management | Unauthorized Change Protection | **CCC-04** | Restrict the unauthorized addition, removal, update, and management of organization assets. |  |
|  | Change Control & Configuration Management | Change Agreements | **CCC-05** | Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs. |  |
|  | Change Control & Configuration Management | Change Management Baseline | **CCC-06** | Establish change management baselines for all relevant authorized changes on organization assets. |  |
|  | Change Control & Configuration Management | Detection of Baseline Deviation | **CCC-07** | Implement detection measures with proactive notification in case of changes deviating from the established baseline. |  |
|  | Change Control & Configuration Management | Exception Management | **CCC-08** | Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process. |  |
|  | Change Control & Configuration Management | Change Restoration | **CCC-09** | Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns. |  |
|  | **Cryptography, Encryption & Key Management** | | | |  |
|  | Cryptography, Encryption & Key Management | Encryption and Key Management Policy and Procedures | **CEK-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually. |  |
|  | Cryptography, Encryption & Key Management | CEK Roles and Responsibilities | **CEK-02** | Define and implement cryptographic, encryption and key management roles and responsibilities. |  |
|  | Cryptography, Encryption & Key Management | Data Encryption | **CEK-03** | Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards. |  |
|  | Cryptography, Encryption & Key Management | Encryption Algorithm | **CEK-04** | Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology. |  |
|  | Cryptography, Encryption & Key Management | Encryption Change Management | **CEK-05** | Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes. |  |
|  | Cryptography, Encryption & Key Management | Encryption Change Cost Benefit Analysis | **CEK-06** | Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. |  |
|  | Cryptography, Encryption & Key Management | Encryption Risk Management | **CEK-07** | Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback. |  |
|  | Cryptography, Encryption & Key Management | CSC Key Management Capability | **CEK-08** | CSPs must provide the capability for CSCs to manage their own data encryption keys. |  |
|  | Cryptography, Encryption & Key Management | Encryption and Key Management Audit | **CEK-09** | Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s). |  |
|  | Cryptography, Encryption & Key Management | Key Generation | **CEK-10** | Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used. |  |
|  | Cryptography, Encryption & Key Management | Key Purpose | **CEK-11** | Manage cryptographic secret and private keys that are provisioned for a unique purpose. |  |
|  | Cryptography, Encryption & Key Management | Key Rotation | **CEK-12** | Rotate cryptographic keys in accordance with the calculated crypto period, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Revocation | **CEK-13** | Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established crypto period, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Destruction | **CEK-14** | Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Activation | **CEK-15** | Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Suspension | **CEK-16** | Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Deactivation | **CEK-17** | Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Archival | **CEK-18** | Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Compromise | **CEK-19** | Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Recovery | **CEK-20** | Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements. |  |
|  | Cryptography, Encryption & Key Management | Key Inventory Management | **CEK-21** | Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements. |  |
|  | **Datacenter Security - DCS** | | | |  |
|  | Datacenter Security | Off-Site Equipment Disposal Policy and Procedures | **DCS-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually. |  |
|  | Datacenter Security | Off-Site Transfer Authorization Policy and Procedures | **DCS-02** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually. |  |
|  | Datacenter Security | Secure Area Policy and Procedures | **DCS-03** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually. |  |
|  | Datacenter Security | Secure Media Transportation Policy and Procedures | **DCS-04** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually. |  |
|  | Datacenter Security | Assets Classification | **DCS-05** | Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. |  |
|  | Datacenter Security | Assets Cataloguing and Tracking | **DCS-06** | Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system. |  |
|  | Datacenter Security | Controlled Access Points | **DCS-07** | Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas. |  |
|  | Datacenter Security | Equipment Identification | **DCS-08** | Use equipment identification as a method for connection authentication. |  |
|  | Datacenter Security | Secure Area Authorization | **DCS-09** | Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization. |  |
|  | Datacenter Security | Surveillance System | **DCS-10** | Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts. |  |
|  | Datacenter Security | Unauthorized Access Response Training | **DCS-11** | Train datacenter personnel to respond to unauthorized ingress or egress attempts. |  |
|  | Datacenter Security | Cabling Security | **DCS-12** | Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms. |  |
|  | Datacenter Security | Environmental Systems | **DCS-13** | Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards. |  |
|  | Datacenter Security | Secure Utilities | **DCS-14** | Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals. |  |
|  | Datacenter Security | Equipment Location | **DCS-15** | Keep business-critical equipment away from locations subject to high probability for environmental risk events. |  |
|  | **Data Security and Privacy Lifecycle Management - DSP** | | | |  |
|  | Data Security & Privacy Lifecycle Management | Security and Privacy Policy and Procedures | **DSP-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually. |  |
|  | Data Security & Privacy Lifecycle Management | Secure Disposal | **DSP-02** | Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means. |  |
|  | Data Security & Privacy Lifecycle Management | Data Inventory | **DSP-03** | Create and maintain a data inventory, at least for any sensitive data and personal data. |  |
|  | Data Security & Privacy Lifecycle Management | Data Classification | **DSP-04** | Classify data according to its type and sensitivity level. |  |
|  | Data Security & Privacy Lifecycle Management | Data Flow Documentation | **DSP-05** | Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change. |  |
|  | Data Security & Privacy Lifecycle Management | Data Ownership and Stewardship | **DSP-06** | Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually. |  |
|  | Data Security & Privacy Lifecycle Management | Data Protection by Design and Default | **DSP-07** | Develop systems, products, and business practices based upon a principle of security by design and industry best practices. |  |
|  | Data Security & Privacy Lifecycle Management | Data Privacy by Design and Default | **DSP-08** | Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations. |  |
|  | Data Security & Privacy Lifecycle Management | Data Protection Impact Assessment | **DSP-09** | Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices. |  |
|  | Data Security & Privacy Lifecycle Management | Sensitive Data Transfer | **DSP-10** | Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations. |  |
|  | Data Security & Privacy Lifecycle Management | Personal Data Access, Reversal, Rectification and Deletion | **DSP-11** | Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations. |  |
|  | Data Security & Privacy Lifecycle Management | Limitation of Purpose in Personal Data Processing | **DSP-12** | Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject. |  |
|  | Data Security & Privacy Lifecycle Management | Personal Data Sub-processing | **DSP-13** | Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations. |  |
|  | Data Security & Privacy Lifecycle Management | Disclosure of Data Sub-processors | **DSP-14** | Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing. |  |
|  | Data Security & Privacy Lifecycle Management | Limitation of Production Data Use | **DSP-15** | Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments. |  |
|  | Data Security & Privacy Lifecycle Management | Data Retention and Deletion | **DSP-16** | Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations. |  |
|  | Data Security & Privacy Lifecycle Management | Sensitive Data Protection | **DSP-17** | Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle. |  |
|  | Data Security & Privacy Lifecycle Management | Disclosure Notification | **DSP-18** | The CSP must 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. The CSP must 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. |  |
|  | Data Security & Privacy Lifecycle Management | Data Location | **DSP-19** | Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up. |  |
|  | **Governance, Risk and Compliance - GRC** | | | |  |
|  | Governance, Risk Management & Compliance | Governance Program Policy and Procedures | **GRC-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually. |  |
|  | Governance, Risk Management & Compliance | Risk Management Program | **GRC-02** | Establish a 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. |  |
|  | Governance, Risk Management & Compliance | Organizational Policy Reviews | **GRC-03** | Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization. |  |
|  | Governance, Risk Management & Compliance | Policy Exception Process | **GRC-04** | Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs. |  |
|  | Governance, Risk Management & Compliance | Information Security Program | **GRC-05** | Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM. |  |
|  | Governance, Risk Management & Compliance | Governance Responsibility Model | **GRC-06** | Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs. |  |
|  | Governance, Risk Management & Compliance | Information System Regulatory Mapping | **GRC-07** | Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. |  |
|  | Governance, Risk Management & Compliance | Special Interest Groups | **GRC-08** | Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context. |  |
|  | **Human Resources - HRS** | | | |  |
|  | Human Resources | Background Screening Policy and Procedures | **HRS-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually. |  |
|  | Human Resources | Acceptable Use of Technology Policy and Procedures | **HRS-02** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually. |  |
|  | Human Resources | Clean Desk Policy and Procedures | **HRS-03** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually. |  |
|  | Human Resources | Remote and Home Working Policy and Procedures | **HRS-04** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually. |  |
|  | Human Resources | Asset returns | **HRS-05** | Establish and document procedures for the return of organization-owned assets by terminated employees. |  |
|  | Human Resources | Employment Termination | **HRS-06** | Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment. |  |
|  | Human Resources | Employment Agreement Process | **HRS-07** | Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets. |  |
|  | Human Resources | Employment Agreement Content | **HRS-08** | The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies. |  |
|  | Human Resources | Personnel Roles and Responsibilities | **HRS-09** | Document and communicate roles and responsibilities of employees, as they relate to information assets and security. |  |
|  | Human Resources | Non-Disclosure Agreements | **HRS-10** | Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details. |  |
|  | Human Resources | Security Awareness Training | **HRS-11** | Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates. |  |
|  | Human Resources | Personal and Sensitive Data Awareness and Training | **HRS-12** | Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization. |  |
|  | Human Resources | Compliance User Responsibility | **HRS-13** | Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory  compliance obligations. |  |
|  | **Identity & Access Management - IAM** | | | |  |
|  | Identity & Access Management | Identity and Access Management Policy and Procedures | **IAM-01** | Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually. |  |
|  | Identity & Access Management | Strong Password Policy and Procedures | **IAM-02** | Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually. |  |
|  | Identity & Access Management | Identity Inventory | **IAM-03** | Manage, store, and review the information of system identities, and level of access. |  |
|  | Identity & Access Management | Separation of Duties | **IAM-04** | Employ the separation of duties principle when implementing information system access. |  |
|  | Identity & Access Management | Least Privilege | **IAM-05** | Employ the least privilege principle when implementing information system access. |  |
|  | Identity & Access Management | User Access Provisioning | **IAM-06** | Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets. |  |
|  | Identity & Access Management | User Access Changes and Revocation | **IAM-07** | De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies. |  |
|  | Identity & Access Management | User Access Review | **IAM-08** | Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance. |  |
|  | Identity & Access Management | Segregation of Privileged Access Roles | **IAM-09** | Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated. |  |
|  | Identity & Access Management | Management of Privileged Access Roles | **IAM-10** | Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access. |  |
|  | Identity & Access Management | CSCs Approval for Agreed Privileged Access Roles | **IAM-11** | Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles. |  |
|  | Identity & Access Management | Safeguard Logs Integrity | **IAM-12** | Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures. |  |
|  | Identity & Access Management | Uniquely Identifiable Users | **IAM-13** | Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs. |  |
|  | Identity & Access Management | Strong Authentication | **IAM-14** | Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities. |  |
|  | Identity & Access Management | Passwords Management | **IAM-15** | Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords. |  |
|  | Identity & Access Management | Authorization Mechanisms | **IAM-16** | Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized. |  |
|  | **Interoperability & Portability - IPY** | | | |  |
|  | Interoperability & Portability | Interoperability and Portability Policy and Procedures | **IPY-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually. |  |
|  | Interoperability & Portability | Application Interface Availability | **IPY-02** | Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability. |  |
|  | Interoperability & Portability | Secure Interoperability and Portability Management | **IPY-03** | Implement cryptographically secure and standardized network protocols for the management, import and export of data. |  |
|  | Interoperability & Portability | Data Portability Contractual Obligations | **IPY-04** | Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy |  |
|  | **Infrastructure & Virtualization Security - IVS** | | | |  |
|  | Infrastructure & Virtualization Security | Infrastructure and Virtualization Security Policy and Procedures | **IVS-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually. |  |
|  | Infrastructure & Virtualization Security | Capacity and Resource Planning | **IVS-02** | Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business. |  |
|  | Infrastructure & Virtualization Security | Network Security | **IVS-03** | Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls. |  |
|  | Infrastructure & Virtualization Security | OS Hardening and Base Controls | **IVS-04** | Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline. |  |
|  | Infrastructure & Virtualization Security | Production and Non-Production Environments | **IVS-05** | Separate production and non-production environments. |  |
|  | Infrastructure & Virtualization Security | Segmentation and Segregation | **IVS-06** | Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants. |  |
|  | Infrastructure & Virtualization Security | Migration to Cloud Environments | **IVS-07** | Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols. |  |
|  | Infrastructure & Virtualization Security | Network Architecture Documentation | **IVS-08** | Identify and document high-risk environments. |  |
|  | Infrastructure & Virtualization Security | Network Defense | **IVS-09** | Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks. |  |
|  | **Logging and Monitoring - LOG** | | | |  |
|  | Logging & Monitoring | Logging and Monitoring Policy and Procedures | **LOG-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually. |  |
|  | Logging & Monitoring | Audit Logs Protection | **LOG-02** | Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs. |  |
|  | Logging & Monitoring | Security Monitoring and Alerting | **LOG-03** | Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics. |  |
|  | Logging & Monitoring | Audit Logs Access and Accountability | **LOG-04** | Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability. |  |
|  | Logging & Monitoring | Audit Logs Monitoring and Response | **LOG-05** | Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies. |  |
|  | Logging & Monitoring | Clock Synchronization | **LOG-06** | Use a reliable time source across all relevant information processing systems. |  |
|  | Logging & Monitoring | Logging Scope | **LOG-07** | Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment. |  |
|  | Logging & Monitoring | Log Records | **LOG-08** | Generate audit records containing relevant security information. |  |
|  | Logging & Monitoring | Log Protection | **LOG-09** | The information system protects audit records from unauthorized access, modification, and deletion. |  |
|  | Logging & Monitoring | Encryption Monitoring and Reporting | **LOG-10** | Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls. |  |
|  | Logging & Monitoring | Transaction/Activity Logging | **LOG-11** | Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys. |  |
|  | Logging & Monitoring | Access Control Logs | **LOG-12** | Monitor and log physical access using an auditable access control system. |  |
|  | Logging & Monitoring | Failures and Anomalies Reporting | **LOG-13** | Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party. |  |
|  | **Security Incident Management, E-Discovery, & Cloud Forensics - SEF** | | | |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Security Incident Management Policy and Procedures | **SEF-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Service Management Policy and Procedures | **SEF-02** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Incident Response Plans | **SEF-03** | Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Incident Response Testing | **SEF-04** | Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Incident Response Metrics | **SEF-05** | Establish and monitor information security incident metrics. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Event Triage Processes | **SEF-06** | Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Security Breach Notification | **SEF-07** | Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations. |  |
|  | Security Incident Management, E-Discovery, & Cloud Forensics | Points of Contact Maintenance | **SEF-08** | Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. |  |
|  | **Supply Chain Management, Transparency, and Accountability - STA** | | | |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Policy and Procedures | **STA-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually. |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Supply Chain | **STA-02** | Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering. |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Guidance | **STA-03** | Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain. |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Control Ownership | **STA-04** | Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering. |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Documentation Review | **STA-05** | Review and validate SSRM documentation for all cloud service~~s~~ offerings the organization uses. |  |
|  | Supply Chain Management, Transparency & Accountability | SSRM Control Implementation | **STA-06** | Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for. |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Inventory | **STA-07** | Develop and maintain an inventory of all supply chain relationships. |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Risk Management | **STA-08** | CSPs periodically review risk factors associated with all organizations within their supply chain. |  |
|  | Supply Chain Management, Transparency & Accountability | Primary Service and Contractual Agreement | **STA-09** | Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Agreement Review | **STA-10** | Review supply chain agreements between CSPs and CSCs at least annually. |  |
|  | Supply Chain Management, Transparency & Accountability | Internal Compliance Testing | **STA-11** | Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually. |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Service Agreement Compliance | **STA-12** | Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards. |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Governance Review | **STA-13** | Periodically review the organization's supply chain partners' IT governance policies and procedures. |  |
|  | Supply Chain Management, Transparency & Accountability | Supply Chain Data Security Assessment | **STA-14** | Define and implement a process for conducting security assessments periodically for all organizations within the supply chain. |  |
|  | **Threat & Vulnerability Management - TVM** | | | |  |
|  | Threat & Vulnerability Management | Threat and Vulnerability Management Policy and Procedures | **TVM-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually. |  |
|  | Threat & Vulnerability Management | Malware Protection Policy and Procedures | **TVM-02** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually. |  |
|  | Threat & Vulnerability Management | Vulnerability Remediation Schedule | **TVM-03** | Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk. |  |
|  | Threat & Vulnerability Management | Detection Updates | **TVM-04** | Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis. |  |
|  | Threat & Vulnerability Management | External Library Vulnerabilities | **TVM-05** | Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy. |  |
|  | Threat & Vulnerability Management | Penetration Testing | **TVM-06** | Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties. |  |
|  | Threat & Vulnerability Management | Vulnerability Identification | **TVM-07** | Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly. |  |
|  | Threat & Vulnerability Management | Vulnerability Prioritization | **TVM-08** | Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. |  |
|  | Threat & Vulnerability Management | Vulnerability Management Reporting | **TVM-09** | Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification. |  |
|  | Threat & Vulnerability Management | Vulnerability Management Metrics | **TVM-10** | Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals. |  |
|  | **Universal Endpoint Management - UEM** | | | |  |
|  | Universal Endpoint Management | Endpoint Devices Policy and Procedures | **UEM-01** | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually. |  |
|  | Universal Endpoint Management | Application and Service Approval | **UEM-02** | Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data. |  |
|  | Universal Endpoint Management | Compatibility | **UEM-03** | Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications. |  |
|  | Universal Endpoint Management | Endpoint Inventory | **UEM-04** | Maintain an inventory of all endpoints used to store and access company data. |  |
|  | Universal Endpoint Management | Endpoint Management | **UEM-05** | Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data. |  |
|  | Universal Endpoint Management | Automatic Lock Screen | **UEM-06** | Configure all relevant interactive-use endpoints to require an automatic lock screen. |  |
|  | Universal Endpoint Management | Operating Systems | **UEM-07** | Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes. |  |
|  | Universal Endpoint Management | Storage Encryption | **UEM-08** | Protect information from unauthorized disclosure on managed endpoint devices with storage encryption. |  |
|  | Universal Endpoint Management | Anti-Malware Detection and Prevention | **UEM-09** | Configure managed endpoints with anti-malware detection and prevention technology and services. |  |
|  | Universal Endpoint Management | Software Firewall | **UEM-10** | Configure managed endpoints with properly configured software firewalls. |  |
|  | Universal Endpoint Management | Data Loss Prevention | **UEM-11** | Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment. |  |
|  | Universal Endpoint Management | Remote Locate | **UEM-12** | Enable remote geo-location capabilities for all managed mobile endpoints. |  |
|  | Universal Endpoint Management | Remote Wipe | **UEM-13** | Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices. |  |
|  | Universal Endpoint Management | Third-Party Endpoint Security Posture | **UEM-14** | Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets. |  |

|  |
| --- |
| **End of Standard** |
| © Copyright 2019-2021 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance “Cloud Controls Matrix (CCM) Version 4.0” at http://www.cloudsecurityalliance.org subject to the following: (a) the Cloud Controls Matrix v4.0 may be used solely for your personal, informational, non-commercial use; (b) the Cloud Controls Matrix v4.0 may not be modified or altered in any way; (c) the Cloud Controls Matrix v4.0 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Cloud Controls Matrix v4.0 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Cloud Controls Matrix Version 4.0. If you are interested in obtaining a license to this material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org. |