CAIQ™

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented,	Yes
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual,	Yes

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

AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes
AIS-03.1	Are technical and operational metrics defined and implemented according to	Yes
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes
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?	Yes

AIS-05.2	Is testing automated when applicable and possible?	Yes
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	No
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes

BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from	Yes
BCR-04.1	Are operational resilience strategies and capability results incorporated	Yes
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business	Yes
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes
BCR-07.1	Do business continuity and resilience procedures establish communication with	Yes

BCR-08.1	Is cloud data periodically backed up?	Yes
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes

BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes
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)?	Yes

CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes
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)?	Yes
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes

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?	Yes
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception	Yes
CCC-09.1	Is a process to proactively roll back changes to a previously known "good	Yes
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes

CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes
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?	Yes

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?	Yes
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?	Yes
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No
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?	Yes
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes

CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	NA
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	NA
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?	NA

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?	NA
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?	NA
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?	NA
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?	NA

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?	NA
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?	Yes
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?	Yes

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?	NA
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?	Yes
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes
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?	Yes

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?	Yes
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes
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?	Yes

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?	Yes
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	NA

DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	NA
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data,	Yes
DCS-07.2	Are physical security perimeters established between administrative and business	Yes
DCS-08.1	Is equipment identification used as a method for connection authentication?	No
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?	Yes
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems	Yes
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress	Yes
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and	Yes
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?	Yes
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned	Yes

DCS-15.1	Is business-critical equipment segregated from locations subject to a high	Yes
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?	Yes
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage	Yes
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes

DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes
DSP-07.1	Are systems, products, and business practices based on security principles	Yes
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal	Yes

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)?	Yes
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and	Yes
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and	Yes
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and	Yes
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and	Yes
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes
DSP-17.1	Are processes, procedures, and technical measures defined and implemented	Yes

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?	Yes
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?	Yes
DSP-19.1	Are processes, procedures, and technical measures defined and implemented	Yes
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes

GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes
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?	Yes
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes
GRC-05.1	Has an information security program (including programs of all relevant CCM	Yes

GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory	Yes
GRC-08.1	Is contact established and maintained with cloud-related special interest	Yes
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?	Yes
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?	Yes

HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes
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?	Yes
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?	Yes

HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes
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?	Yes
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?	Yes
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees	Yes
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes	Yes

HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes
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?	Yes
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes
HRS-11.2	Are regular security awareness training updates provided?	Yes

HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes
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?	Yes
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?	Yes
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes

IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes

IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes
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?	Yes
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?	Yes
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?	Yes
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes

IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes
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?	No
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?	Yes
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?	Yes

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?	Yes
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?	Yes
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes

IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes

IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes

IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes
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	Yes

IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes
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?	Yes
IVS-03.1	Are communications between environments monitored?	Yes
IVS-03.2	Are communications between environments encrypted?	Yes

IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes
IVS-03.4	Are network configurations reviewed at least annually?	Yes
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes
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?	Yes

IVS-05.1	Are production and non-production environments separated?	Yes
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?	Yes
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?	Yes
IVS-08.1	Are high-risk environments identified and documented?	Yes
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?	Yes

LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes

LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes

LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes

LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes

SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes
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?	Yes
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?	Yes
SEF-05.1	Are information security incident metrics established and monitored?	Yes
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes

SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes
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?	Yes

STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	NA
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	NA
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes

STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes
STA-09.1	Do service agreements between CSPs and CSCs (tenants) 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	Yes
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	NA
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?	Yes

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?	Yes
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes
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?	Yes
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes

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

TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	No
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes

UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes
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?	No
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes
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?	Yes

UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	NA

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

End of Standard

SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID
CSP-owned	Liferay maintains comprehensive audit		
CSP-owned	All Liferay security policies and procedures are reviewed annually.		A&A-01
CSP-owned	External/independant audits are performed annually.		A&A-02
CSP-owned	External/independent audits are based on internal risk assessment and risk management priorities determinted by organization leadership.		A&A-03
CSP-owned	Liferay maintains comprehensive audit		A&A-04

CSP-owned	Liferay maintains comprehensive audit polices and procedures to support planning, assessment, corrective actions and review of audit processess.		A&A-05
CSP-owned	Corrective action plans are documentented, implemented and reported as defined in audit policies and procedures.		A&A-06
CSP-owned	Corrective action plans are documentented, implemented and reported as defined in audit policies and procedures.		
CSP-owned	Liferay maintains comprehensive secure development polices and procedures.		AIS-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.	AIS-01
CSP-owned	Liferay maintains comprehensive security baselines for critical systems and services.	AIS-02
CSP-owned	Application security metrics are	AIS-03
CSP-owned	SDLC processes and procedures are implented throughout application life-cycle.	AIS-04
CSP-owned	Application testing procedures factor changes to systems, security requirments and speed of delivery.	AIS-05

CSP-owned	Liferay maintains robust processess and procedures for automated application testing.	AIS-05
CSP-owned	Application development, build and release processess are defined and standardized across organization departments.	AIS-06
CSP-owned	Systems and processess are in place to implement CI/CD pipeline whre possible throughout the SDLC.	
CSP-owned	Liferay maintains and implements vulnerability management and remediation policies and procedures.	AIS-07
CSP-owned	Vulnerability remediation is handled manually, on a case by case basis.	
CSP-owned	Liferay maintains comprehensive Diaster Recovery and Business Continuity polices and procedures.	BCR-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.	BCR-01
CSP-owned	Business continuity and resilence processess and procedures are based on risk assessments performed by senior management.	BCR-02
CSP-owned	Liferay maintains comprehensive	BCR-03
CSP-owned	Liferay maintains comprehensive	BCR-04
CSP-owned	Liferay maintains comprehensive	BCR-05
CSP-owned	Business continuity and resilence processess and procedures are based on risk assessments performed by senior management and available to organization stakeholders.	
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	By policy, recovery procedures are tested and reviewed annually.	BCR-06
CSP-owned	Liferay maintains comprehensive	BCR-07

CSP-owned	Cloud data is periodically backed up.	BCR-08
CSP-owned	Liferay maintains comprehensive Backup polices and procedures which require controls to ensure confidentiality, integrity and availibility.	
CSP-owned	Liferay maintains multifaceted backup mechanisms that include capabilities for disaster recovery of systems and infrastructure.	
CSP-owned	Liferay maintains comprehensive Diaster Recovery and Business Continuity polices and procedures.	BCR-09
CSP-owned	All Liferay security policies and procedures are reviewed annually.	

CSP-owned	By policy, recovery procedures are tested and reviewed annually.	BCR-10
CSP-owned	Liferay maintains relationships with local authorities as part of Business Continuity and Disaster Recovery processess and procedures.	
Shared CSP and 3rd-party	Critical business systems and services are designed with redundancy as per Liferay's Business Continuity and Disater Recovery policies.	BCR-11
CSP-owned	Liferay maintains comprehensive risk management polices and procedures.	CCC-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.	CCC-01
CSP-owned	Change mangement policies and procedures are defined in Liferay's Secure Development and IT Security policies.	CCC-02
CSP-owned	Change mangement policies and procedures take into account risk management processes and procedures as determined by senior management.	CCC-03
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which apply to changes on organization assets and systems.	CCC-04

CSP-owned	Liferay releases are made known to CSC and changes on a schedule.	CCC-05
CSP-owned	Liferay maintains comprehensive security and change management baselines for critical systems and services.	CCC-06
CSP-owned	Liferay maintains a change management system which tests baseline changes.	CCC-07
CSP-owned	Liferay maintains comprehensive risk management polices and procedures.	CCC-08
CSP-owned	Liferay maintains comprehensive risk	
CSP-owned	Liferay maintains comprehensive	CCC-09
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which define baselines for cryptography, encryption and key management.	CEK-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.		CEK-01
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which define key management roles and responsibilities.		CEK-02
CSP-owned	Data in-transit and data at-rest are encrypted using approved cryptographic standards as determined by organization policies and procedures.		CEK-03
CSP-owned	Encryption algorithm standards are determined by organization policies and procedures.		CEK-04
CSP-owned	Changes to critical system components and tooling, including cryptographic and encryption standards must be approved by senior management.		CEK-05

CSP-owned	Liferay has a secure development policy in practice to manage changes to the system, including encryption changes.	CEK-06
CSP-owned	Liferay has risk assements established in our processes to account for this.	CEK-07
CSP-owned	System design and infrastructure is managed by Liferay cloud infrastructure and operations teams.	CEK-08
CSP-owned	All Liferay security policies and procedures are reviewed annually.	CEK-09
CSP-owned	Critical Liferay systems and infrastructure are reviewed annually.	

CSP-owned	Cryptographic and encryption standards, including keys, must be generated using approved standards as defined by policies and procedures.	CEK-10
CSP-owned	System design and infrastructure is managed by Liferay operations teams, private keys and secrets are not for available for management.	CEK-11
CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.	CEK-12
CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.	CEK-13

CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.		CEK-14
CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.		CEK-15
CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.		CEK-16
CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.		CEK-17

CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.	CEK-18
CSP-owned	Liferay maintains comprehensive polices and procedures for encryption implementation.	CEK-19
CSP-owned	Liferay maintains comprehensive polices and procedures for encryption implementation.	CEK-20

CSP-owned	System design and infrastructure is managed by Liferay operations teams, keys are not for available for management.		CEK-21
Shared CSP and 3rd-party	Liferay maintains comprehensive secure disposal polices and procedures. Cloud partner maintains separate disposal policies.		DCS-01
Shared CSP and 3rd-party	Liferay maintains comprehensive secure disposal polices and procedures which require data destruction be performed industry standard destruction procedures.		
CSP-owned	All Liferay security policies and procedures are reviewed annually.		

CSP-owned	Liferay maintains comprehensive system management/IT polices and procedures.	DCS-02
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which apply to changes or transfer of organization assets and systems.	
CSP-owned	All Liferay security policies and procedures are reviewed annually.	

CSP-owned	Liferay maintains comprehensive Physical and Environmental Security polices and procedures.	DCS-03
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
	We do not have physical media.	DCS-04
	We do not have physical media.	
	We do not have physical media.	DCS-05

	We do not have physical media.	DCS-06
Shared CSP and 3rd-	Liferay maintains comprehensive	DCS-07
Shared CSP and 3rd-	Liferay maintains comprehensive	
Shared CSP and 3rd-party	We connect through web based MFA logins to cloud services.	DCS-08
3rd-party outsourced	Liferay's cloud partner manages robust policies and procedures for data center access, physical perimeter, environmental controls and utilities.	DCS-09
CSP-owned	Liferay maintains comprehensive Physical and Environmental Security polices and procedures, including systems and procedures for maintaining security perimeters for physical office locations.	
3rd-party outsourced	Liferay's cloud partner manages	DCS-10
3rd-party outsourced	Liferay's cloud partner manages	DCS-11
3rd-party outsourced	Liferay's cloud partner manages	DCS-12
3rd-party outsourced	Liferay's cloud partner manages robust policies and procedures for data center access, physical perimeter, environmental controls and utilities.	DCS-13
Shared CSP and 3rd-	Liferay maintains comprehensive	DCS-14

Shared CSP and 3rd-	Liferay maintains comprehensive	DCS-15
CSP-owned	Liferay maintains comprehensive Data Classification and handling policies and procedures based on relevant industry, legal and regulatory standards and requirements (e.g. ISO 27K, SOC 2, GDPR, HIPPA)	DSP-01
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	Liferay maintains comprehensive Data	DSP-02
CSP-owned	Liferay maintains comprehensive Data Classification and handling policies and procedures which define sensitivity levels and classification for data types.	DSP-03
CSP-owned	Liferay maintains comprehensive Data	DSP-04
CSP-owned	System and application design documentation is managed by engineeering departments.	DSP-05

CSP-owned	All Liferay security policies and procedures are reviewed annually.	DSP-05
CSP-owned	Liferay maintains comprehensive Information Classification and Data Retention polices and procedures.	DSP-06
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	Liferay maintains comprehensive	DSP-07
CSP-owned	Liferay maintains comprehensive Information Security polices and procedures which apply security and privacy best practice to organization systems, processes and practices.	DSP-08
CSP-owned	Liferay maintains comprehensive Information Security polices and procedures which apply security and privacy best practice to organization systems, processes and practices.	
CSP-owned	Liferay's Data Privacy Office	DSP-09

CSP-owned	Liferay's Data Privacy Office maintains policies and procedures which take into account industry best practice and regulatory requirements. Additonally Liferay maintains Information Classifcation and data handling policies which apply to data access and processing.		DSP-10
CSP-owned	Liferay's Data Privacy Office		DSP-11
CSP-owned	Liferay's Data Privacy Office		DSP-12
CSP-owned	Liferay's Data Privacy Office		DSP-13
CSP-owned	Liferay's Data Privacy Office		DSP-14
CSP-owned	Per policy clients must be informed and consent prior to the transference of production data to non-production or testing systems.		DSP-15
CSP-owned	Liferay maintains comprehensive Information Classification and Data Retention polices and procedures based on applicable laws, regulation and industry standards.		DSP-16
CSP-owned	Liferay maintains comprehensive		DSP-17

CSP-owned	In the event of data request by law enforcement, Data Privacy Office and senior management would handle procedures on case by case basis per applicable laws and regulations.	DSP-18
CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	
Shared CSP and 3rd-	Liferay maintains comprehensive	DSP-19
CSP-owned	Liferay maintains comprehensive Information Security polices and procedures which are sponsored and approved by organization leadership and management.	GRC-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.	GRC-01
CSP-owned	Liferay maintains comprehensive Information Security and Risk Management polices and procedures which are sponsored and approved by organization leadership and management.	GRC-02
CSP-owned	All Liferay security policies and procedures are reviewed annually.	GRC-03
CSP-owned	Liferay maintains comprehensive Corrective Action polices and procedures in the event of non-conformities to security program policies.	GRC-04
CSP-owned	Liferay maintains a comprehensive	GRC-05

CSP-owned	Liferay maintains a comprehensive Information Security Management Systems, including defined roles and responsibilities within the security program.		GRC-06
CSP-owned	Liferay maintains a comprehensive		GRC-07
Shared CSP and 3rd-	Liferay recognizes the important role		GRC-08
CSP-owned	All Liferay employees must undergo background verification processess, as possible based on local laws and regulation and per organization policies.		HRS-01
CSP-owned	All Liferay employees must undergo background verification processess, as possible based on local laws and regulation.		

CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which define and implement acceptable use for organization assets.	HRS-02
CSP-owned	All Liferay security policies and procedures are reviewed annually.	

CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which define and implement acceptable use for organization assets including clean desk requirements.	HRS-03
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	Liferay maintains comprehensive IT Security polices and procedures which define and implement acceptable use for organization assets, including use of assets from remote sites.	HRS-04
CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	Liferay maintains comprehensive IT	HRS-05
CSP-owned	Liferay maintains comprehensive	HRS-06

CSP-owned	All Liferay employees must sign employement agreement prior to accessing organization systems.		HRS-07
CSP-owned	All Liferay employees must sign employement agreement which require acceptance of security responsbilities.		HRS-08
CSP-owned	All Liferay employees must sign employement agreement which define employee role and responsibilities.		HRS-09
CSP-owned	All Liferay employees must sign employement agreement which define confidentiality within the employee role and responsibilities.		HRS-10
CSP-owned	All Liferay employees must take an annual security awarenesss training based on employee role and responsibilities.		HRS-11
CSP-owned	All Liferay security policies and procedures are reviewed annually.		

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually.		HRS-12
CSP-owned	Liferay requires all employees to retake the privacy and security awareness training annaully. The trainings content are reviewed and updated accordingly on an annual basis.		
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. In addition, Liferay has an Code of Conduct which addresses responsibilities and expected behavior with respect to the protection of		HRS-13
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes access control		IAM-01

CSP-owned	All Liferay security policies and procedures are reviewed annually.		IAM-01
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes password procedures.		IAM-02
CSP-owned	All Liferay security policies and procedures are reviewed annually.		
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. Access control is reviewed		IAM-03
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes		IAM-04
CSP-owned	Liferay has a need-to-know policy based on roles, using the concept of least privilege to match access privileges to defined responsibilities.		IAM-05

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes separation of duties for information		IAM-06
CSP-owned	Lieray has established provisioning and de-provisioning policies and processes in place within our Information Security Management System.		IAM-07
CSP-owned	Liferay has a access review performed at least annually. This reviews can result in improvements or action items.		IAM-08
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes separation of duties for information access.		IAM-09
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes separation of duties for information		IAM-10

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes separation of duties for information	IAM-10
CSP-owned	The customers access is part of the product. Participation is not available.	IAM-11
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes varies log access implementations.	IAM-12
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes varies log access implementations.	

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes varies log access implementations.		IAM-13
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes varies log access implementations.		IAM-14
CSP-owned	Liferay systems can include deigital certificates in limited capacity.		
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes		IAM-15

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes	IAM-16
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes secure development policies.	
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes secure development policies.	

CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes secure development policies.		IPY-01
CSP-owned	Liferay has established a information security and privacy training program and requires all employees to complete this training upon hire and annually. The program includes secure development policies.		

CSP-owned	All Liferay security policies and procedures are reviewed annually.	
CSP-owned	The data source is available to CSC.	IPY-02
CSP-owned	Network protocols are encrypted.	IPY-03
CSP-owned	CSC can request data based on contract terms.	IPY-04

CSP-owned	Infrastructure is continuely getting upgrades.	IVS-01
CSP-owned	Reviewed annually.	
CSP-owned	Part of our service offerings.	IVS-02
CSP-owned	As part of the infrastructure.	
CSP-owned	Communication between environments are encrypted.	

CSP-owned	Access controls in place between environments.	IVS-03
CSP-owned	Reviewed annually.	
CSP-owned	Configurations documented.	
Shared CSP and 3rd-party	Cloud vendor provided environment are all tested by CSP	IVS-04

CSP-owned	Prod and non-prod environments are separated.	IVS-05
CSP-owned	CSC tenent is separated by CSP with other tenents.	IVS-06
CSP-owned	CSP used cloud vendor protocols.	IVS-07
CSP-owned	Risk analysis include environment reviews.	IVS-08
CSP-owned	Network protections are documented.	IVS-09

CSP-owned	Documented and part of service offerings.	LOG-01
CSP-owned	Reviewed annually.	
CSP-owned	Reviewed annually.	LOG-02
CSP-owned	CSP monitored.	LOG-03
CSP-owned	CSP implemented process.	

CSP-owned	CSP implemented process.	LOG-04
CSP-owned	CSP implemented process.	LOG-05
CSP-owned	CSP implemented process.	
CSP-owned	We implemented with cloud vendor's time source.	LOG-06
CSP-owned	CSP implemented process.	LOG-07

CSP-owned	Reviewed annually.	LOG-07
CSP-owned	CSP implemented process.	LOG-08
CSP-owned	Access controls in place between environments.	LOG-09
CSP-owned	Liferay maintains comprehensive polices and procedures for encryption implementation.	LOG-10
CSP-owned	Liferay maintains comprehensive polices and procedures for encryption implementation.	LOG-11
3rd-party outsourced	Physical access maintained by our cloud vendor	LOG-12

CSP-owned	CSP implemented process.	LOG-13
CSP-owned	CSP implemented process.	
CSP-owned	CSP implemented process.	SEF-01
CSP-owned	Reviewed annually.	
CSP-owned	CSP implemented process.	SEF-02

CSP-owned	Reviewed annually.	SEF-02
CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	SEF-03
CSP-owned	Reviewed annually.	SEF-04
CSP-owned	CSP implemented process.	SEF-05
CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	SEF-06

CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	SEF-07
CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	
CSP-owned	CSP implemented process.	SEF-08
CSP-owned	Liferay maintains comprehensive Incident Response and Notification Procedures polices and procedures.	STA-01

CSP-owned	Reviewed annually.	STA-01
Shared CSP and 3rd-party	CSP implemented process.	STA-02
	CSC is not given SSRM guidance from CSP.	STA-03
	No shared ownership.	STA-04
CSP-owned	CSP used cloud vendor protocols.	STA-05
Shared CSP and 3rd-party	Cloud vendor evaluated by CSP.	STA-06

CSP-owned	CSP implemented process.	STA-07
CSP-owned	External/independent audits are based on internal risk assessment and risk management priorities determinted by organization leadership.	STA-08
CSP-owned	CSP implemented process.	STA-09
CSP-owned	There are no supply chain agreements between CSPs and CSCs.	STA-10
CSP-owned	Reviewed annually.	STA-11

CSP-owned	CSP implemented process.	STA-12
CSP-owned	REviewed annually.	STA-13
CSP-owned	CSP implemented process.	STA-14
CSP-owned	Liferay maintains and implements vulnerability management and remediation policies and procedures.	TVM-01
CSP-owned	Reviewed annually.	

CSP-owned	CSP implemented process.	TVM-02
CSP-owned	Reviewed annually.	
CSP-owned	CSP implemented process.	TVM-03
CSP-owned	CSP implemented process.	TVM-04
CSP-owned	CSP implemented process.	TVM-05

CSP-owned	CSP implemented process.	TVM-06
CSP-owned	Vulnerability remediation is handled manually, on a case by case basis.	TVM-07
CSP-owned	CSP implemented process.	TVM-08
CSP-owned	Liferay maintains and implements vulnerability management and remediation policies and procedures.	TVM-09
CSP-owned	CSP implemented process.	TVM-10
CSP-owned	CSP implemented process.	UEM-01

CSP-owned	Reviewed annually.	UEM-01
CSP-owned	Liferay InfoSec does not consider this a risk to the company.	UEM-02
CSP-owned	Endpoints are available for all devices.	UEM-03
CSP-owned	Liferay uses tools available for inventory.	UEM-04
CSP-owned	CSP implemented process.	UEM-05

CSP-owned	CSP implemented process.	UEM-06
CSP-owned	CSP implemented process.	UEM-07
CSP-owned	CSP implemented process.	UEM-08
CSP-owned	CSP implemented process.	UEM-09
CSP-owned	Endpoints are available for all devices.	UEM-10
CSP-owned	Endpoints do not contain data to be lost.	UEM-11
CSP-owned	Mobile endpoints are not enabled.	UEM-12

CSP-owned	Mobile endpoints are not enabled.	UEM-13
CSP-owned	Third party endpoints do not have access to our organizational assets.	UEM-14

CCM Control Specification	CCM Control Title
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 and Assurance Policy and Procedures
Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments
Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment
Verify compliance with all relevant standards, regulations, legal/contractual,	Requirements Compliance

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 Management Process
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.	Remediation
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 and Interface Security Policy and

	Security Policy and Procedures
Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements
Define and implement technical and operational metrics in alignment	Application Security Metrics
Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development
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.	Automated Application

	Security Testing
Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment
Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation
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 Policy and

	Management Policy and Procedures
Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis
Establish strategies to reduce the impact of, withstand, and recover	Business Continuity
Establish, document, approve, communicate, apply, evaluate and maintain	Business Continuity
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.	Documentation
Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises
Establish communication with stakeholders and participants in the	Communication

Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup
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.	Disaster Response Plan

Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise
Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy
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 Management Policy

	and Procedures
Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing
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 Management Technology
Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection

Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements
Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline
Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation
'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.'	Exception Management
Define and implement a process to proactively roll back changes to	Change Restoration
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.	Encryption and Key Management Policy and

	Management Policy and Procedures
Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities
Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption
Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm
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.	Encryption Change Management

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.	Encryption Change Cost Benefit Analysis
Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management
CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability
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).	Encryption and Key Management Audit

Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation
Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose
Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation
Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation

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.	Key Destruction
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.	Key Activation
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.	Key Suspension
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.	Key Deactivation

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.	Key Archival
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.	Key Compromise
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.	Key Recovery

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.	Key Inventory Management
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.	Off-Site Equipment Disposal Policy and Procedures

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.	Off-Site Transfer Authorization Policy and Procedures

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.	Secure Area Policy and Procedures
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.	Secure Media Transportation Policy and Procedures
Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification

Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking
Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the	Controlled Access Points
Use equipment identification as a method for connection authentication.	Equipment Identification
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.	Secure Area Authorization
Implement, maintain, and operate datacenter surveillance systems	Surveillance System
Train datacenter personnel to respond to unauthorized ingress or	Unauthorized Access
Define, implement and evaluate processes, procedures and technical	Cabling Security
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.	Environmental Systems
Secure, monitor, maintain, and test utilities services for continual	Secure Utilities

Keep business-critical equipment away from locations subject to high	Equipment Location
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.	Security and Privacy Policy and Procedures
Apply industry accepted methods for the secure disposal of data from	Secure Disposal
Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory
Classify data according to its type and sensitivity level.	Data Classification
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 Flow Documentation

	Data Flow Documentation
Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship
Develop systems, products, and business practices based upon a principle	Data Protection by Design
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 Privacy by Design and Default
Conduct a Data Protection Impact Assessment (DPIA) to evaluate the	Data Protection Impact

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.	Sensitive Data Transfer
Define and implement, processes, procedures and technical measures	Personal Data Access,
Define, implement and evaluate processes, procedures and technical	Limitation of Purpose in
Define, implement and evaluate processes, procedures and technical	Personal Data Sub-
Define, implement and evaluate processes, procedures and technical	Disclosure of Data Sub-
Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use
Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion
Define and implement, processes, procedures and technical measures	Sensitive Data Protection

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.	Disclosure Notification
Define and implement, processes, procedures and technical measures	Data Location
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 Program Policy

	and Procedures
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.	Risk Management Program
Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews
Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process
Develop and implement an Information Security Program, which includes	Information Security

Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model
Identify and document all relevant standards, regulations, legal/contractual,	Information System
Establish and maintain contact with cloud-related special interest	Special Interest Groups
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.	Background Screening Policy and Procedures

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.	Acceptable Use of Technology Policy and Procedures

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.	Clean Desk Policy and Procedures
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.	Remote and Home Working Policy and Procedures
Establish and document procedures for the return of organization-owned	Asset returns
Establish, document, and communicate to all personnel the procedures	Employment Termination

Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process
The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content
Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities
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.	Non-Disclosure Agreements
Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training

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.	Personal and Sensitive Data Awareness and Training
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.	Compliance User Responsibility
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 and Access Management Policy and

	Management Policy and Procedures
Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures
Manage, store, and review the information of system identities, and level of access.	Identity Inventory
Employ the separation of duties principle when implementing information system access.	Separation of Duties
Employ the least privilege principle when implementing information system access.	Least Privilege

Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning
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.	User Access Changes and Revocation
Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review
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.	Segregation of Privileged Access Roles
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.	Management of Privileged

	Access Roles
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.	CSCs Approval for Agreed Privileged Access Roles
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.	Safeguard Logs Integrity

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.	Uniquely Identifiable Users
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.	Strong Authentication
Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management

Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms
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 and Portability Policy and Procedures

Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability
Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management
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	Data Portability Contractual Obligations

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 and Virtualization Security Policy and Procedures
Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning
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.	

	Network Security
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.	OS Hardening and Base Controls

Separate production and non-production environments.	Production and Non-Production Environments
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.	Segmentation and Segregation
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.	Migration to Cloud Environments
Identify and document high-risk environments.	Network Architecture Documentation
Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense

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 and Monitoring Policy and Procedures
Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection
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.	Security Monitoring and Alerting

Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability
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.	Audit Logs Monitoring and Response
Use a reliable time source across all relevant information processing systems.	Clock Synchronization
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 Scope

	Logging Scope
Generate audit records containing relevant security information.	Log Records
The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection
Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting
Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging
Monitor and log physical access using an auditable access control system.	Access Control Logs

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.	Failures and Anomalies Reporting
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 Policy and Procedures
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.	Service Management Policy

	and Procedures
'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.'	Incident Response Plans
Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing
Establish and monitor information security incident metrics.	Incident Response Metrics
Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes

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 Breach Notification
Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance
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.	SSRM Policy and Procedures

	SSRM Policy and Procedures
Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain
Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance
Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership
Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review
Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation

Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory
CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management
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	Primary Service and Contractual Agreement
Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review
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.	Internal Compliance Testing

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 Service Agreement Compliance
Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review
Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment
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 and Vulnerability Management Policy and Procedures

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.	Malware Protection Policy and Procedures
Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule
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.	Detection Updates
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.	External Library Vulnerabilities

Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing
Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification
Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization
Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting
Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics
Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and

	Procedures
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.	Application and Service Approval
Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility
Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory
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.	Endpoint Management

Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen
Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems
Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption
Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention
Configure managed endpoints with properly configured software firewalls.	Software Firewall
Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention
Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate

Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe
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.	Third-Party Endpoint Security Posture

CCM Domain Title
Audit & A

Audit & Assurance

Application & Interface Security

Business Continuity Management and Operational Resilience

Change Control and Configuration Management

Cryptography, Encryption & Key Management

Datacenter Security

Data Security and Privacy Lifecycle Management

Governance, Risk and Compliance

Human Resources

Identity & Access
Management

Interoperability &
Portability

Infrastructure & Virtualization Security

Logging and Monitoring

Security Incident Management, E-Discovery, & Cloud Forensics

Supply Chain Management, Transparency, and Accountability

Threat & Vulnerability Management

Universal Endpoint Management