CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes		Exalate is ISO 27001:2022 certified. Compliance is verified at least once a year through internal and external audits				A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	Audit & Assurance
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes						A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes		Exalate is ISO 27001:2022 certified. Compliance is verified at least once a year through internal and external audits				A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes		In line ISO 27001:2022 requirements							
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes						AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	Application & Interface Security
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes						AIS-04	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	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes						AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
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		In line ISO 27001:2022 requirements				AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes									
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements				BCR-01		Management Policy and Procedures	Business Continuity Management and Operational Resilience
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes		In line ISO 27001:2022 requirements				BCR-02	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	
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes						BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-08.1	Is cloud data periodically backed up?	Yes						BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
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		In line ISO 27001:2022 requirements				BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes		In line ISO 27001:2022 requirements							
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		In line ISO 27001:2022 requirements				CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements				CCC-01		and Procedures	Change Control and Configuration Management
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes		In line ISO 27001:2022 requirements				CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes						CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
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		Contract with Cloud Provider make sure we are compliant				CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes		As defined in Change Management Policy				CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes		As defined in Change Management Policy				CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes		As defined in Change Management Policy				CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes						CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes						CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes						CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	Cryptography, Encryption & Key Management
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-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
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-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes						CEK-12	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	
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?	Yes						CEK-13	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	
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?	Yes						CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
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		In line ISO 27001:2022 requirements				DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	Datacenter Security
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes		In line ISO 27001:2022 requirements				DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes		In line ISO 27001:2022 requirements				DCS-06	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	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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		In line ISO 27001:2022 requirements, GDPR				DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	Data Security and Privacy Lifecycle Management
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes		In line with EU GDRP requirements				DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes		In line with EU GDRP requirements				DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes		In line with EU GDRP requirements				DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes		In line ISO 27001:2022 requirements							
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes						DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
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 by design and per industry best practices?	Yes						DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes						DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes		In line with EU GDRP requirements							

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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		In line with EU GDRP requirements				DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes		In line with EU GDRP requirements				DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes		In line with EU GDRP requirements				DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes		In line with EU GDRP requirements				DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes		In line with EU GDRP requirements				DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes						DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes						DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes						DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements				GRC-01		and Procedures	Governance, Risk and Compliance
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		In line ISO 27001:2022 requirements				GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes						GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes		In line ISO 27001:2022 requirements				GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	Human Resources
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
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		In line ISO 27001:2022 requirements				HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures	
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		In line ISO 27001:2022 requirements							
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	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	
HRS-11.2	Are regular security awareness training updates provided?	Yes		Staff are required to participate in security training at least once a year							

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	Identity & Access Management
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes						IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes						IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes						IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes						IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
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-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
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		At least once a year. Business critical application are reviewed more frequently				IAM-08	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	
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-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
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	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	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes									

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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		In line ISO 27001:2022 requirements				IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	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	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	Interoperability & Portability
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									

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
IVS-03.1	Are communications between environments monitored?	Yes						IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	Infrastructure & Virtualization Security
IVS-03.2	Are communications between environments encrypted?	Yes		SSL TLS is used							
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-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
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-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
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						IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	Logging and Monitoring
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes						LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes						LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes		In line ISO 27001:2022 requirements							
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		In line ISO 27001:2022 requirements				SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	Security Incident Management, E-Discovery, & Cloud Forensics
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		In line ISO 27001:2022 requirements				SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes		In line ISO 27001:2022 requirements				SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	

CAIQ Lite **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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		In line with EU GDRP requirements				SEF-07		Security Breach Notification	
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes		In line with EU GDRP requirements				STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	Supply Chain Management, Transparency, and Accountability
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes		In line with EU GDRP requirements				STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes						STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes		In line ISO 27001:2022 requirements				TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	Threat & Vulnerability Management
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes		In line ISO 27001:2022 requirements							
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-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
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-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes						TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes						TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
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?	Yes						UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	

CAIQ Lite CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE LITE v4.0.3

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes						UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	Universal Endpoint Management
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-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes						UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes						UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes						UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes						UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	

End of Standard

© Copyright 2024 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire Lite (CAIQLite) Version 4.0.3" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire Lite v4.0.3 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire Lite v4.0.3 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire Lite Version 4.0.3. If you are interested in obtaining a license to this #material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.