CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

This tab includes the questionnaire associated with the Cloud Control Matrix (CCM) controls, commonly known as the CAIQ.

The Consensus Assessments Initiative Questionnaire version 4 (or CAIQv4.0.2) aligns with the CCMv4.0.2 control specifications. The CAIQv4.0.2's purpose is to help organizations conduct self-assessments to test their compliance against the CCM V4. It is developed under CSA's STAR-Level 1 program umbrella, allowing organizations to complete and submit self-assessments to CSA's STAR Registry.

The CAIQv4.0.2 features 261 questions structured and formulated based on the 17 domains and underlying control specifications of the CCM.

Each question is described using the following attributes:

Question ID

The question identifiers.

Assessment Question

The description of the question.

In addition, this tab includes the following sections (groups of columns).

CSP CAIQ Answer

The Cloud Service Provider (CSP) must respond with “Yes”/ ”No”/ ”NA” next to the corresponding assessment question, and for the portion(s) of the CCM control specification they are responsible and accountable for implementing.

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

Meaning of possible replies:

• “Yes”: The portion(s) of the CCM control requirement corresponding to the assessment question is met.

• “No”: The portion(s) of the CCM control requirement corresponding to the assessment question is not met.

• “N/A”: The question is not in scope and does not apply to the cloud service under assessment.

NOTES:

A “Yes” answer indicates that the portion of the control in question is implemented. The CSP indicates the responsible and accountable parties (SSRM control ownership), and optionally elaborates on the implementation “how-to” per relevant party CSP and/or CSC.

A “No” answer indicates that the portion of the control in question is not implemented, while in scope of the assessment. The CSP has to assign the implementation responsibility of the control to the relevant party under column “SSRM control ownership”, and optionally elaborate on the “why” (has not been implemented), and “what” has to be done for its implementation by that party.

A “N/A” answer indicates that the portion of the control in question is out of scope of the assessment. The “SSRM control ownership” column is to be left blank (e.g., greyed out), and optionally the CSP may explain why it is the case (“CSP Implementation Description”).

Shared Security Responsibility Model (SSRM) control ownership

The CSP control responses shall identify control applicability and ownership for their specific service.

• CSP-owned: The CSP is entirely responsible and accountable for the CCM control implementation.

• CSC-owned: The Cloud Service Customer (CSC) is entirely responsible and accountable for the CCM control implementation.

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

• Third-party outsourced: The third-party CSP in the supply chain (e.g., an IaaS provider) is responsible for CCM control implementation, while the CSP is fully accountable.

• Shared CSP and CSC: Both the CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is shared between CSP and the third party, but the CSP remains fully accountable.

Note: The CAIQv4 SSRM schema is tailored to CCMv4's Supply Chain Management, Transparency, and Accountability (STA) domain, controls 1-6, and their corresponding implementation guidelines.

CSP implementation description (optional/recommended)

A description (with references) of how the cloud service provider meets (or does not meet) the portion(s) of the SSRM control they are responsible for. If "NA," explain why.

CSC responsibilities (optional/recommended)

A summary description of the cloud service customer security responsibilities for the portion(s) of the SSRM control that is responsible for, with corresponding guidance and references.

End of Introduction

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The organization operates according to policies aligned to ISO 27001. In particular, the internal controls are subject to an independent third party audit and an internal audit, and relate to the stated scope of ISO 27001:2013 certification.				A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	Annually; audit and assurance assessments are conducted by a certification body in order to maintaine and kept up-to-date our ISO 27001 certification.				A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	Performed as part of ISO 27001:2013 standard certification.				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	CSP-owned	Performed as part of ISO 27001:2013 standard certification.				A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
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	CSP-owned	Performed as part of ISO 27001:2013 standard certification.				A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Performed as part of ISO 27001:2013 standard certification.				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	CSP-owned								
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	3rd-party outsourced	The application security policies are covered by SaaS Vendor.				AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	3rd-party outsourced	The application security policies are managed by SaaS Vendor.							
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	3rd-party outsourced	The application security policies are managed by SaaS Vendor.				AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	No						AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	3rd-party outsourced	The SDLC process is defined and implemented by SaaS Vendor.				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-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?	No						AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
AIS-05.2	Is testing automated when applicable and possible?	No						AIS-05		Security Testing	
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	No						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	3rd-party outsourced	The the automation of deployment and integration of application code is implemented by SaaS Vendor.							
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	3rd-party outsourced	The processes to remediate application security vulnerabilities are defined by SaaS Vendor.				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?	No									
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The Organization operates under policies that are ISO 27001 aligned. In particular Present has developed and mantains a framework for business continuity and disaster recovery, with the exclusion of Data Center services which are IaaS provider responsability.				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 Procedures	Business Continuity Management and Operational Resilience
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes)							
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	It is based on risk management procedure and policy established according to ISO 27001:2013 standard certification.				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	CSP-owned	It is based on risk management procedure and policy established according to ISO 27001:2013 standard certification.				BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	It is based on risk management procedure and policy established according to ISO 27001:2013 standard certification.				BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned					BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Since BC documentation is classified as "confidential", disclosure is permitted only if confidential agreements are established, even with authorized stakeholders.							
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes)							
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	BC plan is tested at planned intervals or based on major changes occured to the ISMS (infrastructure, organization or context changes).				BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned					BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	CSP-owned	It is based on risk management procedure and policy established according to ISO 27001:2013 standard certification. The backup is related only on application and envoronmental data. No personal or sensitive data is backed-up					Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.		

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-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	NA						BCR-08		Backup	
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and 3rd-party	The organization, with the support of SaaS Vendor, can restore the backups of application data for resilency.							
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	CSP-owned	DRP is part of BC process.				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	CSP-owned	DRP plan is updated annually or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	DRP plan is tested at planned intervals or based on major changes occured to the ISMS (infrastructure, organization or context changes).				BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
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	Shared CSP and 3rd-party					BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
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	CSP-owned	The changes to be made to the organizational assets like hardware, software and infrastructure resources are managed through a change management process supported by specific tools and procedures.				CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are updated annually or based on major changes occured to the ISMS (infrastructure, hardware and software changes).							
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	No						CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
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	CSP-owned	Changes to supplier services are managed through timely reviews by the relevant corporate functions, taking into account applicable security requirements. Where necessary, a new risk analysis is carried out to document and mitigate any new risks.				CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	The organization has defined access control rules with reference to general logical and physical security policies. These rules are periodically reviewed				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?	No						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	

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-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned					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?	No						CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	The organization has established a policy as part of ISMS.				CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	No									
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	CSP-owned	A rollback process is part of the 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	CSP-owned	Cryptography, encryption and key management policies are part of the organization's ISO 27001:2013 certification and they are applied only to systems for which the requirements are met.				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	CSP-owned	Policies and procedures are updated annually or based on major changes occured to the ISMS (infrastructure, hardware and software changes).							
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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	
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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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-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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-09		Management Audit	Cryptography, Encryption & Key Management
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not				CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				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	
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		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
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		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
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		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
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		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	
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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
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?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	

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-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		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization data encryption is not required.				CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	Datacenter Security
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
DCS-08.1	Is equipment identification used as a method for connection authentication?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of				DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
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	CSP-owned	The Organization operates under policies that are ISO 27001 aligned. In particular Present has developed and mantains policies to address information classification schemes, specifying the information useful and necessary for classification, protection and management throughout the entire life cycle in accordance with regulations, standards and risk levels.				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	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are updated annually or based on major changes occured to the ISMS							

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	Data Security and Privacy Lifecycle Management
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization .				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.							
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.							
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.							
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
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)?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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)?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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)?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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-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)?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the				DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the				DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
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?	NA		For the purpose of the questionnaire the question is not applicable, since no data handling regarding sensitive and personal data is performed within the service managed by the organization.				DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification	
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	CSP-owned								
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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	CSP-owned	Present's ISMS policy is aimed at ensuring the company's conduct in protecting the integrity, confidentiality and availability of its customers' information assets, processed within the scope of its service provision business, through the continuous improvement of its organizational capabilities, in compliance with the binding requirements of the reference regulatory framework. The policy consists of a set of guidelines and procedures that form an integral part of it. The established policies and procedures are approved and communicated to the appropriate levels of the organization.				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 and Procedures	
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							

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-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	CSP-owned	Risk Management processesss are established and implemented based on ISO 27001 requirements. DPIA and BIA are defined also inside the Company's Risk Management framework.				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	Governance, Risk and Compliance
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).				GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	No						GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	An Information Security Program is established, approved and maintained on annual basis.				GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	The organization has clearly identified and described the internal roles involved in information security management and their associated responsibilities. More than one role may be associated with the same person and a role may be split between several people.				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	CSP-owned	The set of regulations, laws and standards applicable to the context of the organization are identified by the relevant department, which also takes advice from business associations. In addition, the contractual documents signed with customers include the security requirements to be maintained for the duration of the service contract.				GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned					GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	
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	CSP-owned	The organization has implemented a selection and recruitment process that involves checking specific personal and professional requirements of candidates. The extent of the screening process (Criminal Background Checking) is, however, commensurate with the sensitivity of the information to be processed (data classification to be accessed) and the nature of the job (business				HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
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	CSP-owned								
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (organization or context changes).							
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	CSP-owned	The organization has defined and maintains policies and procedures to regulate the correct use of IT assets, including their classification and control.				HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and	

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
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	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).				HRS-02		Technology Policy and Procedures	Human Resources
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The organization has defined both appropriate policies and, within the framework of an "education package", the appropriate behaviours for the management of one's own workspce, in particular when it is abandoned, both in work activities and at the end of the day.				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	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (organization or context changes).							
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	CSP-owned	The use of IT devices, and the consequent management of information outside company premises, is governed by security provisions set out both policies and individual assignment letters.				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	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	The organization has defined procedures to regulate: a) the return of IT assets and the management of deletion of users/revision of authorisation levels in the event of resignation or change of job of the employee; b) the management procedures of ISMS documents, in case of deletion (obsolescence) or changes (versioning); c) the management of the ISMS documents, in case of deletion (obsolescence) or				HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Whenever there is a change of employment, the new roles and responsibilities, including in terms of information security, are discussed with the employee.				HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	The organization has defined the contractual documentation to be given to the new employee, based on the type of employment relationship. These documents include instructions on his or her information security responsibilities, such as: letter of appointment for personal data processing, Code of Conduct and Business Ethics, Security and use of work tools (PC, Smartphone, etc.) , etc.				HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned					HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned					HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
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	CSP-owned	All new employees sign a Confidentiality Agreement during their onboarding process.				HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	

CAIQ

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	The organization has defined a 'Security education package' with the aim of informing and describing the correct behaviour to guarantee and safeguard the security and protection of both company and customer information assets. Training is also provided for both new and existing staff, with periodic refresher sessions through an e-learning platform. In particular, the "Awareness" platform includes the simulation of social engineering attacks (phishing) and special e-learning modules with the in-depth analysis of specific social media risks inside the organization.				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	CSP-owned	Information security training sessions are applied by the organization at six-month intervals.							
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	The e-learning platform also includes the Personal Data Protection (GDPR) module and the trainiong course is delivered to all employees of the organization.				HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training	
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	CSP-owned	Procedures, processes and policies are regularly updated based on major changes occured to the ISMS (reflecting changes in the organization, regulations, legal and context).							
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	CSP-owned	Employees sign a confidentiality agreement committing them to protect confidential information they may become aware during emplyment.				HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	The organization leverages on Access Control Policy and Information Security Policy to manage the control policies for registration, management and removal of digital identities.				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	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	The organization leverages on Access Control Policy and Information Security Policy to manage the control policies for registration, management and removal of digital identities.				IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	The organization leverages on Access Control Policy and Information Security Policy to manage the control policies for registration, management and removal of digital identities.				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	CSP-owned	The organization has defined Operational Procedure to manage the separation of duties.				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	CSP-owned	The organization has defined Operational Procedure to manage the least privilege principle.				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	CSP-owned	The organization reviews the Access Control List and Roles as needed for asset access changes.				IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	

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-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	CSP-owned	The organization reviews the Access Control List and Roles as needed for asset access changes.				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	Identity & Access Management
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	CSP-owned	The organization reviews the Access Control List and Roles in according to performed Risk Analyis .				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?	No						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	Shared CSP and 3rd-party	The organization leverages on Access Control Systems of SaaS Provider to accomplish the requirement.				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?	No									
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?	NA						IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
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?	No						IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
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?	No									
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?	No						IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
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?	No						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?	No									
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	No						IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	No						IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	

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-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	No						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?	No									
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	No									
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	No									
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	No									
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	3rd-party outsourced	The solution developed by SaaS Vendor enebles interoperability and portability via API.				IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	No						IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
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	CSP-owned	The organization defines provisions specifying CSC access to data upon contract termination.				IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							

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-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	Shared CSP and 3rd-party	The organization leverages on 3rd parties IaaS and uses SaaS solution monitoring tools.				IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	Infrastructure & Virtualization Security
IVS-03.1	Are communications between environments monitored?	No						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	
IVS-03.2	Are communications between environments encrypted?	Yes	3rd-party outsourced	The communications versus the SaaS Vendor solution are encrypted (SSL/TLS).							
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	3rd-party outsourced	The access to console SaaS Vendor solution is enforced by the least privilege concept.							
IVS-03.4	Are network configurations reviewed at least annually?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.							
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	No									
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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-05.1	Are production and non-production environments separated?	Yes	3rd-party outsourced	The SaaS Vendor has implemented the separation between produtction and non-production environment.				IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
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	3rd-party outsourced	The SaaS Vendor has segmented, segregated, monitored and restricted the user and the intra-tenant access.				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	
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned					IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
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?	NA		The terms of controls are covered in contracts between SaaS and IaaS Provider, with differences in base of the used IaaS.				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	CSP-owned	Logging and Monitoring Policy are part of the organization's ISO 27001:2013 certification and they are applied only to systems for which the requirements are met.				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	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are updated annually or based on major changes occured to the ISMS (infrastructure, hardware and software changes).				LOG-01		Policy and Procedures	Logging and Monitoring
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	NA		For the purpose of the questionnaire the question is not applicable, since within the service managed by the organization audit log security and retention are not required.				LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	NA						LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	NA									
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	NA						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?	NA						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?	NA									
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	NA						LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	NA						LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	NA									
LOG-08.1	Are audit records generated, and do they contain relevant security information?	NA						LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	NA						LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	NA						LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	NA						LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	NA						LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	NA						LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies	

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
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	NA						LOG-13		Reporting	
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	CSP-owned	The organization maintains incident response procedures as part of Information Security Incident Management Policy as part of ISO 27001:2013 standard certification.				SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The organization maintains incident response procedures as part of Information Security Incident Management Policy as part of ISO 27001:2013 standard certification.				SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
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	CSP-owned	The organization maintains incident response procedures as part of Information Security Incident Management Policy as part of ISO 27001:2013 standard certification.				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	
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	CSP-owned	The organization maintains incident response procedures as part of Information Security Incident Management Policy as part of ISO 27001:2013 standard certification.				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-05.1	Are information security incident metrics established and monitored?	Yes	Shared CSP and 3rd-party	Both the organization and the SaaS Vendor have established and monitored security incident metrics.				SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	Shared CSP and 3rd-party	Both the organization and SaaS Vendor report processes, procedures and technical mesaures in the Security Incident Respons Plan				SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	Shared CSP and 3rd-party	Both the organization and SaaS Vendor report processes, procedures and technical mesaures in the Security Incident Respons Plan				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	
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	CSP-owned	Security Incident Response Plan is part of ISO 27001:2013							
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	The organization reports the points of contact in the Security Incident Respons Plan				SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	
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	Shared CSP and 3rd-party					STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	Shared CSP and 3rd-party								

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	Shared CSP and 3rd-party					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-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	Shared CSP and CSC					STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
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	Shared CSP and 3rd-party					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-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	Shared CSP and 3rd-party					STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	Shared CSP and 3rd-party					STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	Shared CSP and 3rd-party					STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	Shared CSP and 3rd-party	The risk factors are reviewed on major changes occured within the Supply Chain.				STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
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	Shared CSP and CSC					STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	Shared CSP and CSC	The supply chain agreements are eventually reviewed based on quality and results of the delivered service				STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
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	Shared CSP and CSC					STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
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	CSP-owned	The requirements are covered by contractual documentation.				STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned					STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	No						STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
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	Shared CSP and 3rd-party	Both the organization and SaaS Vendor manage policies and processes, as requested in the requirement.				TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	Both the organization and SaaS Vendor review and update policies and processes,.							

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

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
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned					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	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
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	3rd-party outsourced	The SaaS Vendor manage policies, processes and technical measures to enable scheduled and emergnecy responses to vulnerabilty identifications.				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?	No						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-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	3rd-party outsourced	The SaaS Vendor defines, implements and evaluates processes, procedures and technical mesaures.				TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned					TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	
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-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-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	3rd-party outsourced	The SaaS Vendor prioritizes vulnerability remediation using a risk based model.				TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	No						TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	3rd-party outsourced	The SaaS Vendor establishes, monitors and reports the metrics for vunlerability identification and remediation.				TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	The organization program, processes and procedures to manage antivirus / malicious software are aligned with ISO27001 standard.				UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	During annual ISO 27001 re-certification process or based on major changes occured to the ISMS (infrastructure, organization or context changes).							
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	CSP-owned	Each Delivery Unit centralizes these informations and is responsable for the proper use of the approved list of services and applications.				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	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned					UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned					UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	

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-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	CSP-owned					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	Universal Endpoint Management
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned					UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned					UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned					UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned					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	CSP-owned					UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	No						UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No						UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	No						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	
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?	Yes	CSP-owned	The contractual mesaures are implemented and evaluated.				UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	

End of Standard