CAIQ™

GUARDINEX
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	CSC-owned		We have formal policies and procedures that cover information security, secure software development, vendor management, risk management, BCP, data classification and retention, vulnerability management, etc. There are also policies for code of conduct and acceptable use. All personnel are required to review and acknowledge these policies/procedures, and undergo required training. The goal is to comply with applicable laws and regulations, as well as industry standards that are appropriate for the business (such as SOC 2, ISO27001, GDPR, CCPA, etc)		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSC-owned		Internal audits/assessments are performed periodically, and an external audit is conducted annually by an independent CPA. The auditors reported is made available to Customers/Partners on demand. The goal of the audits/assessments is to validate the implementation and effectiveness of required Controls.		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	CSC-owned		A formal Risk Management policy is implemented, and audited as part of the annual external audit, as well as periodic internal audits.		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	CSC-owned		All regulatory requirements, legal requirements, contractual requirements, industry standards are implemented through policies and controls, and verified by the internal and external audits.		A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-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	CSC-owned		Audits, reviews, and procedures that need to happen on a schedule are automated in a dedicated calendar that is shared with the compliance team. The controls implemented include, but are not limited to SOC 2 (all 5 TSC criteria - Security, Availability, Confidentiality, Privacy, Processing integrity)		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	CSC-owned		There is a risk management program that is described in a formal policy document. As part of that, we maintain a risk register that is reviewed periodically and atleast once annually. The management team, as part of a Review process, assesses risks and plans remediation every quarter.		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	CSC-owned		A risk register is maintained to track the status of each risk, and communicated to relevant stakeholders. The Risk Management program includes a periodic review process when new risks are evaluated and registered, and existing risks in the register are reviewed for remediation. This risk register is shared with all relevant stakeholders.					
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	CSC-owned		We have formal policies and procedures that cover information security, and secure software development. These cover measures for application security, network security, data security. All personnel are required to review and acknowledge these policies/procedures, and undergo required training.		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	
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Each policy is reviewed atleast annually, as part of the Management Review process					
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSC-owned		Our development process adheres to the formal software development policy that includes a security assessment, use of security hardened baseline configurations, design reviews, code reviews, and continuous static and dynamic security scans.		AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	

CAIQ

GUARDINEX

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-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSC-owned		a) Application code scan generates metrics for bugs, vulnerabilities, hotspots. We monitor and maintain these metrics, with a requirement to remediate all of them. b) Application dynamic scan generates low/med/high alerts. We monitor and ensure med/high alerts are remediated. c) Cloud logs are monitored with queries, that generate an alarm whenever there is a security event (e.g. access denied to a resource) d) Source code tools automatically monitor the code base for vulnerabilities in various dependent modules and provides vulnerability alerts		AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	Application & Interface Security
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSC-owned		Our development process adheres to the formal software development policy that includes a security assessment, use of security hardened baseline configurations, design reviews, code reviews, and continuous static and dynamic security scans.		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?	Yes	CSC-owned		Every change that is pushed to code repository automatically triggers a security scan of the code, and metrics are collected and available for analytics and remediation of bugs, vulnerabilities, hotspots identified. Every deployment automatically triggers a dynamic security scan of the application and findings are sent over email to the security response team, which works on mitigating any issues identified. Every deployment also automatically triggers functional tests, results of which are sent over email to the development team, which works on mitigating issues identified.		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 Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSC-owned		Code changes cannot be merged to the main trunk until they passes automated unit tests, and are approved by a reviewer. Every change that is pushed to code repository automatically triggers a security scan of the code, and metrics are collected and available for analytics and remediation of bugs, vulnerabilities, hotspots identified. Every deployment automatically triggers a dynamic security scan of the application and findings are sent over email to the security response team, which works on mitigating any issues identified. Every deployment also automatically triggers functional tests, results of which are sent over email to the development team, which works on mitigating issues identified.					
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSC-owned		Code changes cannot be merged to the main trunk until they passes automated unit tests, and are approved by a reviewer. Deployment is automated, and it automatically triggers functional tests and a security scan of the deployed application. The results of the tests and security scan are emailed to the dev and security teams respectively for remediation. Before any changes are deployed to production, there are 3 phases of deployment and test - to a developers local machine, to a development environment in the cloud, and to a staging environment in the cloud.		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	CSC-owned		Code changes cannot be merged to the main trunk until they passes automated unit tests, and are approved by a reviewer. Deployment is automated, and it automatically triggers functional tests and a security scan of the deployed application. The results of the tests and security scan are emailed to the dev and security teams respectively for remediation. Before any changes are deployed to production, there are 3 phases of deployment and test - to a developers local machine, to a development environment in the cloud, and to a staging environment in the cloud.					

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-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSC-owned		Every change that is pushed to code repository automatically triggers a security scan of the code, and metrics are collected and available for analytics and remediation of bugs, vulnerabilities, hotspots identified. Every deployment automatically triggers a dynamic security scan of the application and findings are sent over email to the security response team, which works on mitigating any issues identified.		AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSC-owned		Every change that is pushed to code repository automatically triggers a security scan of the code, and metrics are collected and available for analytics and remediation of bugs, vulnerabilities, hotspots identified. Every deployment automatically triggers a dynamic security scan of the application and findings are sent over email to the security response team, which works on mitigating any issues identified.					
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned		We have a BCP/DR plan that covers planned/unplanned outages, data backup/retention, communication, testing of the plan, and the 4 phases of handling a disaster (Identification, Response, Recovery, Learning)		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSC-owned		The response phase of our BCP/DR plan performs an impact assessment to determines what team members, facilities and customer deployments are affected by the disaster scenario and in what way they are affected. The response phase also considers actions to mitigate the impact as much as possible before a final solution is in place.		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	CSC-owned		The recovery phase of our BCP/DR plan conducts activities necessary to bring the business back to normal, with cost and effort incurred being proportional to the risk posed by the disaster		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	CSC-owned		We have a BCP/DR plan that covers planned/unplanned outages, data backup/retention, communication, testing of the plan, and the 4 phases of handling a disaster (Identification, Response, Recovery, Learning)		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	CSC-owned		We have a BCP/DR plan that covers planned/unplanned outages, data backup/retention, communication, testing of the plan, and the 4 phases of handling a disaster (Identification, Response, Recovery, Learning)		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	CSC-owned		We have a BCP/DR plan that covers planned/unplanned outages, data backup/retention, communication, testing of the plan, and the 4 phases of handling a disaster (Identification, Response, Recovery, Learning) This plan is reviewed and acknowledged by all personnel and made available to partners/customers on demand.					
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSC-owned		The BCP/DR plan test is part of the schedule for business processes and occurs at an annual cadence. The plan is also reviewed and modified as part of the learnings phase of handling a disaster.		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	CSC-owned		Communication with affected stakeholders and BCP/DR team participants is an integral part of the BCP/DR plan		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	CSC-owned		Database data is automatically backed up on a daily basis			Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup		

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?	Yes	Shared CSP and CSC		Our CSP ensures the availability and integrity of the backups. We ensure confidentiality by configuring the backups to be encrypted		BCR-08	for resiliency.	Backup	
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSC-owned		Database data can be restored with an RTO of a few hours and a RPO of within a few minutes before the disaster					
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	CSC-owned		We have a BCP/DR plan that covers planned/unplanned outages, data backup/retention, communication, testing of the plan, and the 4 phases of handling a disaster (Identification, Response, Recovery, Learning)		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process The BCP/DR plan is also reviewed and modified as part of the learnings phase of handling a disaster.					
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSC-owned		The BCP/DR plan test is part of the schedule for business processes and occurs at an annual cadence. The plan is also reviewed and modified as part of the learnings phase of handling a disaster.		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?	Yes	CSC-owned		Communication with affected stakeholders and BCP/DR team participants is an integral part of the BCP/DR plan, and local emergency authorities are stakeholders for certain disasters (e.g. a fire)					
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 CSC		All our business critical equipment is in the cloud. The CSP ensures redundancy of the equipment while we ensure that all layers of the cloud stack utilize designs that avoid a single point of failure. Resilient architecture is an inherent requirement		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	CSC-owned		We have an explicit policy to manage change. A change to production goes through the following process. 1. Infosec review is conducted for proposed change 2. code related to the change is tracked in a development ticket 3. Infosec review is conducted for the implementation 4. change is tested on a developer's local environment, and in the cloud on a dev environment, followed by a staging environment 5. change goes through static and dynamic security testing 6. change is design reviewed and code reviewed 7. change to production is registered in a change ticket in which the following is documented: a) change type - normal/standard/emergency b) impact c) urgency d) risk e) reason f) implementation plan g) test plan h) rollback plan 8. the change ticket is reviewed and approved 9. the change is pushed to production For emergency changes (characterized in the policy), a notification is sent to the manager, change is applied to mitigate the emergency. Following that, a change ticket is created, and the change is revisited and reviewed to ensure the change had no adverse impact on security, stability, and functionality		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSC-owned		See response to CCC-01.1		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	CSC-owned		See response to CCC-01.1		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	

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-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSC-owned		Changes need to be approved before they are applied to production. The permissions to apply changes to production are granted only to specific personnel (principle of least privilege)		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?	NA	CSP-owned		Yes. We have agreements with our CSP in the role as a CSC. We have agreements with our CSCs (customers) in the role as a CSP.		CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSC-owned		See response to CCC-01.1		CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSC-owned		See response to CCC-01.1		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	CSC-owned		See response to CCC-01.1		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?'	Yes	CSC-owned		See response to CCC-01.1					
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	CSC-owned		See response to CCC-01.1		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	Shared CSP and CSC		We have an explicit policy for encryption and key management. This policy defines minimum requirements for strong encryption (TLS 1.2+), encryption of data at rest and in transit, and secure management of keys (generation, storage, rotation). The policy also discusses encryption requirements, over and above the transport encryption, of confidential data that is transmitted between parties. The cryptography algorithms used are guided by NIST security requirements. The CSP provides support for secure transport protocols and secure cryptography algorithms approved by NIST		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSC-owned		See response to CEK-01.1		CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSC-owned		See response to CEK-01.1		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?	Yes	CSC-owned		See response to CEK-01.1		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	

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-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSC-owned		See response to CEK-01.1 and CCC-01.1. Change management policy encompasses changes in the domain of encryption and key management.		CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	Cryptography, Encryption & Key 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?	Yes	CSC-owned		See response to CEK-01.1 and CCC-01.1. Change management policy encompasses changes in the domain of encryption and key management.		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?	Yes	CSC-owned		Our compliance program includes Information Security policies and procedures, a Security incident response plan, and Risk management. These have been described in response to earlier questions		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?	Yes	Shared CSP and CSC		The CSP provides support for secure transport protocols and secure cryptography algorithms approved by NIST		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?	Yes	CSC-owned		Internal audits/assessments are performed periodically, and an external audit is conducted annually by an independent CPA. The goal of the audits/assessments is to validate the implementation and effectiveness of required Controls. The security incident response plan includes recovery and learning phases which ensure that gaps are addressed to prevent future recurrence		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 Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSC-owned		Internal audits/assessments are performed periodically, and an external audit is conducted annually by an independent CPA. The goal of the audits/assessments is to validate the implementation and effectiveness of required Controls.					
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and CSC		The CSP provides support for secure transport protocols and secure cryptography algorithms approved by NIST		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?	Yes	CSC-owned		Separate keys are provisioned for separate uses (encrypting files, databases, credentials) and mechanisms provided by the CSP for key management are used		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?	Yes	Shared CSP and CSC		The CSP's key management service includes the ability to rotate keys at a schedule determined by the CSC		CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC		The CSP's key management service includes the ability to revoke keys, which is used when appropriate (e.g. security incident due to compromise of keys, or personnel with access to keys leave the organization)		CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and CSC		The CSP's key management service is used exclusively for key management. It provides the ability to destroy keys or revoke key access. This facility is used when needed.		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	

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-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?	Yes	Shared CSP and CSC		The CSP's key management service has the ability to create pre-activated keys but we do not use such a facility		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?	Yes	Shared CSP and CSC		The CSP's key management service has the ability to disable keys, which is used when appropriate		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?	Yes	Shared CSP and CSC		The CSP's key management service has the ability to disable keys, which is used when appropriate		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?	Yes	Shared CSP and CSC		The CSP's keymanagement service does not provide an explicit mechanism to archive keys but it provides the ability to disable keys and manage access policies. This is used as an archiving mechanism for keys. In other words, the keys to be archived are kept in the service itself and not in a separate archive		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?	Yes	Shared CSP and CSC		The CSP's key management service is used for data encryption/decryption in a way that we never have to worry about compromised keys or to recover lost keys. A key-encryption-key (KEK) is used whose cryptographic material never leaves the key management service. This KEK is used to dynamically generate a new data key for each encryption. The plaintext data key is only in memory and never saved anywhere. The encrypted data and the encrypted key is then saved in the ciphertext.		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?	Yes	Shared CSP and CSC		The CSP's key management service is used for data encryption/decryption in a way that we never have to worry about compromised keys or to recover lost keys. A key-encryption-key (KEK) is used whose cryptographic material never leaves the key management service. This KEK is used to dynamically generate a new data key for each encryption. The plaintext data key is only in memory and never saved anywhere. The encrypted data and the encrypted key is then saved in the ciphertext.		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	
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?	Yes	Shared CSP and CSC		The CSP's key management service provides APIs and UI to manage the inventory of Keys		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?	Yes	CSP-owned		We have no offsite equipment. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					

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-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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	Datacenter Security
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP					

CAIQ

GUARDINEX
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-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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?	Yes	CSP-owned		We have no offsite equipment, no server rooms, no data centers. We use the CSP for our infrastructure. This responsibility is owned by the CSP		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	CSC-owned		We have policies that cover the following: - data retention and disposal as per laws and contractual obligations - data classification as per sensitivity level to ensure fine-grained access controls on data - information security to keep data secure - risk management to handle data related risks and incidents		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned		CSPs are responsible for ensuring the removal of data from disks before they are repurposed and before the destruction of decommissioned hardware. CSP uses media sanitization guidelines by NIST		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	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSC-owned		Assets are inventoried and are reviewed periodically, and atleast once annually		DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSC-owned		See response to DSP-01.1		DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSC-owned		Data flow and storage across all systems and accounts is always maintained up to date, and is reviewed every quarter		DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSC-owned		Data flow and storage across all systems and accounts is always maintained up to date, and is reviewed every quarter					

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-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSC-owned		Data across all systems and accounts is maintained in a regularly updated document, and is reviewed every quarter		DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	Data Security and Privacy Lifecycle Management
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSC-owned		It is reviewed every quarter					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSC-owned		Our information security policy mandates that data is always encrypted at rest and in transit. It also mandates access controls on the principle of least privilege. Our encryption and key management policy specifies encryption requirements for transfer of confidential data between individuals or groups. Applications that access data are tested, developed and deployed as per the secure software development policy. The policy requires that security assessment and review is conducted for every change, and security testing is done for every change.		DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSC-owned		Our privacy policy requires a privacy impact assessment for every new engagement with partners or customers. The policy requires the upholding of data subject fundamental rights as specified by privacy standards. The privacy compliance program ensures periodic reviews and assessments to ensure adherence to controls.		DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSC-owned		See response to DSP-08.1					
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?	Yes	CSC-owned		See response to DSP-08.1		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)?	Yes	CSC-owned		Our information security policy mandates that data is always encrypted at rest and in transit. It also mandates access controls on the principle of least privilege. Our encryption and key management policy specifies encryption requirements for transfer of confidential data between individuals or groups. Contracts signed with customers include a "permitted use" section that mandates that we use data as mutually agreed and above all in accordance with laws, regulations and industry standards		DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSC-owned		Our privacy policy requires the upholding of data subject fundamental rights as specified by privacy standards. These rights include: Right to be informed Right to access Right to rectification Right to erasure Right to restrict processing Right to data portability Right to object Right in relation to automated decision making and profiling		DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSC-owned		Contracts signed with customers include a "permitted use" section that mandates that we use data as mutually agreed and above all in accordance with laws, regulations and industry standards		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™

GUARDINEX
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)?	Yes	CSC-owned		We sign contracts with customers and downstream data partners that have clauses on confidentiality and permitted use. The clauses stipulate that we use data as mutually agreed and above all in accordance with laws, regulations and industry standards	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSC-owned		We sign contracts with customers and downstream data partners that have clauses on confidentiality and permitted use. The clauses stipulate that we use data as mutually agreed and above all in accordance with laws, regulations and industry standards	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?	Yes	CSC-owned		Non-production environments never use production data, they only use fake (generated) PII data	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?	Yes	CSC-owned		We have a data retention and disposal policy that requries the following: The time period for which we retain data from customers and data partners depends on the purpose for which it is used. We retain such data for as long as an account is active or in accordance with the agreement(s) with the customer or data partner, unless required by law or regulation to dispose of data earlier or retain data longer. Data is safely disposed as and when required by contracts and the law.	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSC-owned		The information security policy requires that sensitive data is stored and disposed of, in a manner that; reasonably safeguards the confidentiality of the data (by encrypting it at rest and in transit); protects against the unauthorized use or disclosure of the data; and renders the data secure or appropriately destroyed	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?	Yes	Shared CSP and CSC		The information security policy and the privacy policy require that personal data is protected from any unauthorized access and disclosure. All our policies require that we conform with applicable laws. Any requests for disclosure by Law Enforcement are handled in accordance with the law.	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	Shared CSP and CSC		We do not receive Personal Data directly from individuals. We receive it from our business customers and partners. Our agreements with them stipulate that both parties handle the data in accordance with the law.				
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSC-owned		A document that describes the data flow and storage across all systems and accounts is always maintained up to date, and is reviewed every quarter	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	CSC-owned		We have formal policies and procedures that cover information security, secure software development, vendor management, risk management, BCP, data classification and retention, vulnerability management, etc. There are also policies for code of conduct and acceptable use. All personnel are required to review and acknowledge these policies/procedures, and undergo required training. The goal is to comply with applicable laws and regulations, as well as industry standards that are appropriate for the business (such as SOC 2, ISO27001, GDPR, CCPA, etc)	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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process				

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	CSC-owned		We have a risk management program describe in the risk assessment and treatment policy. There is an assessment framework that identifies, tracks, handles and assess risks periodicallly.		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process		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?	Yes	CSC-owned		Every policy includes an exception section. Our business needs, local situations, laws and regulations may occasionally call for an exception to any policy. If an exception is needed, management will determine an acceptable alternative approach.		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	CSC-owned		We have an information security program described in the information security policy. This covers all aspects of security in our company. - People security: background checks, confidentiality agreements, training - Physical security - Access security - Asset security - Data security, retention, disposal - Change management - Secure Development - Vulnerability management - BCP/DR - Incident Response - Vendor management - Risk management Many of these aspects are also covered in separate dedicated policies and designates specific roles and responsibilities to implement the controls		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	CSC-owned		See response to GRC-05.1		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	CSC-owned		A legal compliance policy requires us to maintain a Legal Compliance Register that tracks all relevant statutory, regulatory, contractual requirements and the organization's approach to meet these requirements. This register also keeps track of compliance status and gaps if any. The policy also specifies a process for a new legal requirement		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	CSC-owned		Personnel are part of various professional groups/communities (e.g. Stackoverflow, dev. to) for the purpose of learning, sharing knowledge about Development, Security, Privacy, Technology trends, etc.		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	CSC-owned		Our policies require background checks on all candidates for employment (including contractors) in accordance with relevant local laws, regulations and ethics and are performed in accordance with the business requirements, the classification of the information to be accessed and the perceived risks. Our information security policy lists the background checks required.		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	CSC-owned		See response to HRS-01.1					

CAIQ

GUARDINEX

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-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					Human Resources
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	CSC-owned		Our acceptable use policy specifies responsibilities of personnel related to use of communication tools, personal mobile devices, social media, and handling of company assets including data		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 Procedures	
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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned		See response to HRS-02.1		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
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	CSC-owned		Our information security policy specifically addresses Remote Work and requires use of secure protocols to protect data and credentials in transit. It also has guidelines on working in public spaces and from home. We employ the principle of least privilege when granting access to any personnel, and conduct an access review every quarter. Access to sensitive systems requires strong passwords and multi-factor authentication.		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. We track all onboarding, offboarding, access change in a ticketing system, with formal approvals and respective checklists detailing activities to be completed.		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	CSC-owned		See response to HRS-05.1		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	CSC-owned		All employees sign an employment agreement prior to starting employment. All employees are also required to review and accept all our policies, and the acknowledgement is recorded. As and when there are policy changes, employees are automatically asked to review the changes and accept them.		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	CSC-owned		The employment agreement includes clauses on handling confidential information, compliance with company policies and use of company equipment and facilities, and returning company assets on termination		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	CSC-owned		The employment agreement and the policies that employees are required to accept detail the responsibilities of employees with respect to company assets, including data		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	

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-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	CSC-owned		The employment agreement includes clauses on confidentiality and non-disclosure		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	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSC-owned		Our information security policy requires that all employees undergo security awareness and compliance training, and the policy has a list of trainings and respective periodicity of repeating the training.		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSC-owned		There is a periodicity (typically annual) with which employees are required to go through training, including security awareness training					
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSC-owned		All employees are required to complete security awareness training regardless of whether they have access to sensitive data		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	CSC-owned		When employees onboard, they review and accept all policies, and their acceptance is recorded. They also complete requisite training. After that, whenever there is an update to any policy, employees are automatically notified to review and accept the changes. This is for all employees regardless of whether they have access to sensitive data					
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	CSC-owned		See response to HRS-12.2		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	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. Employees are granted access, based on approvals, on a need basis, in keeping with the principle of least privilege.		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSC-owned		Our information security policy specifically addresses password security - including secrecy, complexity, rotation and storing of passwords. Password complexity requirements are included in the access control and termination policy.		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSC-owned		Access reviews are conducted every quarter. This includes a review of all critical systems, principals who have access and their access level, and whether the access is commensurate with business requirements		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	CSC-owned		Access is only granted to a system if a principal requires access as part of the job responsibilities. We strongly adhere to role based access control, and employ the concept of Groups and assign Roles to Groups where available. This makes access management more flexible and secure		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	CSC-owned		We strongly adhere to the principle of least privilege, and assign access and level only as required by business. In addition, access to sensitive systems requires an additional factor for authentication (MFA)		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	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. We track all onboarding, offboarding, access change in a ticketing system, with formal approvals and respective checklists detailing activities to be completed.		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	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. We track all onboarding, offboarding, access change in a ticketing system, with formal approvals and respective checklists detailing activities to be completed.		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	CSC-owned		Access reviews are conducted every quarter. This includes a review of all critical systems, principals who have access and their access level, and whether the access is commensurate with business requirements		IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSC-owned		Access is only granted to a system if a principal requires access as part of the job responsibilities. We strongly adhere to role based access control, and employ the concept of Groups and assign Roles to Groups where available. This makes access management more flexible and secure		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	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. We track all onboarding, offboarding, access change in a ticketing system, with formal approvals and respective checklists detailing activities to be completed. Privileged access is also managed using the same process. When there is a change in job duties/role, a ticket is created to implement changes in access required. This ensures access for all personnel is maintained only at the level required by a job function.		IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSC-owned		See response to IAM-10.1					
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	No			Customers are never granted privileged access to systems		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?	Yes	CSC-owned		Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. System and user activity logs may be utilized to assess the causes of incidents and problems. Guardinex utilizes access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information. Logs from infrastructure and application are gathered into dedicated log gathering services. The infrastructure and the application are assigned the ability to write to these systems. Access to log gathering service is limited to administrator only, and even the administrator cannot modify the logs. These logs are used for generating alerts on anomalous conditions, for diagnosing system problems and for viewing dashboards for specific component logs. We use a specific log gathering service for runtime exceptions in the application. These logs are used for diagnosing runtime problems by developers. These logs cannot be modified.		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?	Yes	CSC-owned		There is no provision to modify the logs once they are generated. Logging configuration can only be modified by an administrator. Also see response to IAM-12.1					

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-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSC-owned		All access goes through authentication and authorization. Each accessing Principal gets unique authentication credentials. Authorization is provided through roles, that are attached permissions just enough to fulfill job responsibilities. If additional permissions are required, they are added after a change ticket for additional access is approved.		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?	Yes	CSC-owned		Our access control and termination policy specifies the procedures for onboarding and offboarding personnel, as well as changes to access. We track all onboarding, offboarding, access change in a ticketing system, with formal approvals and respective checklists detailing activities to be completed. We strongly adhere to the principle of least privilege, and assign access and level only as required by business. In addition, access to sensitive systems requires an additional factor for authentication (MFA)		IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSC-owned		All network communication in the system uses Secure Transport only (TLS 1.2+) and all servers therefore have digital certificates for authentication. For customer access to the application, client digital certificates for strong authentication are also supported					
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSC-owned		Our information security policy specifically addresses password security - including secrecy, complexity, rotation and storing of passwords. Password complexity requirements are included in the access control and termination policy.		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?	Yes	CSC-owned		All access goes through authentication and authorization. Each accessing Principal gets unique authentication credentials. Authorization is provided through roles, that are attached permissions just enough to fulfill job responsibilities. If additional permissions are required, they are added after a change ticket for additional access is approved. Access is monitored and anomalous activities generate alerts.		IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSC-owned		Our API is documented on a public site. Applications use published CSP APIs that are well documented		IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSC-owned		Our API is documented on a public site. Applications use published CSP APIs that are well documented					
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSC-owned		Our API is documented on a public site. Applications use published CSP APIs that are well documented					
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSC-owned		Our API is documented on a public site. Applications use published CSP APIs that are well documented					
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned		Applications use published CSP APIs that are well documented		IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	

GUARDINEX
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
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSC-owned		Only Secure transport (TLS 1.2+) is used for all network communications which ensures data is encrypted in transit with strong ciphers and servers are authenticated with digital certificates.		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	CSC-owned		We have policies that cover data retention and disposal as per laws and contractual obligations The time period for which we retain data from customers and data partners depends on the purpose for which it is used. We retain such data for as long as an account is active or in accordance with the agreement(s) with the customer or data partner, unless required by law or regulation to dispose of data earlier or retain data longer. Data is safely disposed as and when required by contracts and the law.		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?	Yes	CSC-owned		We have formal policies and procedures that cover information security, network security and secure software development. All personnel are required to review and acknowledge these policies/procedures, and undergo required training. The goal is to comply with applicable laws and regulations, as well as industry standards that are appropriate for the business (such as SOC 2, ISO27001, GDPR, CCPA, etc)		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	Infrastructure & Virtualization Security
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
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	CSC-owned		The entire application stack is on the cloud and adheres to the design principle of elastic scaling, and high availability. No manual intervention is required for capacity management and system availability. Systems and Networks are monitored for security or performance events. When such events occur, notifications are sent automatically to personnel and remedial action is taken		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	
IVS-03.1	Are communications between environments monitored?	Yes	CSC-owned		Systems and Networks are monitored for security or performance events. When such events occur, notifications are sent automatically to personnel and remedial action is taken		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	CSC-owned		Only Secure transport (TLS 1.2+) is used for all network communications which ensures data is encrypted in transit with strong ciphers and servers are authenticated with digital certificates.					
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSC-owned		All access - machine to machine or human to machine - goes through authentication and authorization. Each accessing Principal gets unique authentication / authorization credentials. Authorization is provided through roles, that are attached permissions just enough to fulfill job responsibilities. If additional permissions are required, they are added after a change ticket for additional access is approved. Access is monitored and anomalous activities generate alerts.					
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSC-owned		Network Review, Firewall Review, and Access Review is performed every quarter. This is in addition to application security scans that are performed on every deployment (and therefore several times a month)					
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSC-owned		All access - machine to machine or human to machine - goes through authentication and authorization. Each accessing Principal gets unique authentication / authorization credentials. Authorization is provided through roles, that are attached permissions just enough to fulfill job responsibilities. If additional permissions are required, they are added after a change ticket for additional access is approved. Access is monitored and anomalous activities generate alerts.					

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-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and CSC		CSP and Guardinex have a shared responsibility where CSP takes care of the hypervisor and OS configuration, and Guardinex takes care of application configuration. We use CSP provided hardened OS images and follow our configuration and asset management policy to ensure secure configurations.		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	CSC-owned		Production and non-production environments have a hard separation by virtue of provisioning in separate CSP accounts, with no cross account access.		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	Shared CSP and CSC		CSP takes care of tenant segragation at the infrastructure level. Guardinex takes care of segregating customer data and access at the application level.		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	CSC-owned		We have no use case for migrating to the cloud. Our genesis was in the cloud.		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	CSC-owned		We have a Network Security policy which we adhere to. We review our network architecture every quarter. Our network design places application components in private subnets, except those that provide a public interface. Firewall review is also conducted every quarter to ensure proper network segmentation		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?	Yes	CSC-owned		We use CSP-provided intrusion detection systems, and monitoring for threats and anomalous events. We have policies for Network Security, Information Security, and Incident Response that specify controls and actions to be taken.		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	CSC-owned		Our information security policy covers logging and monitoring. We collect & monitor audit logs and alerts on key events stemming from infrastructure and applications, as well as IAM user and admin activities. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts. Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. We utilize access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information. When events and alerts are generated, we correlate those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy. Additionally, we utilize threat detection solution(s) to actively monitor and alert on network and application-based threats.		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					

CAIQ™

GUARDINEX
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-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSC-owned		Our information security policy covers logging and monitoring. Logs are securely stored and archived for a minimum of 1 year to assist with potential forensic efforts. Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. We utilize access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.		LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	Logging and Monitoring
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSC-owned		Our information security policy covers logging and monitoring. When events and alerts are generated, we correlate those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy.		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?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We collect & monitor audit logs and alerts on key events stemming from infrastructure and applications, as well as IAM user and admin activities. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines. When events and alerts are generated, we correlate those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy.					
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSC-owned		Our information security policy covers logging and monitoring. Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. We utilize access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.		LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines. When events and alerts are generated, we correlate those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy.		LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines.					
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSC-owned		All systems utilize the NTP network time daemon to keep their clocks synchronized		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?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We collect & monitor audit logs and alerts on key events stemming from infrastructure and applications, as well as IAM user and admin activities.		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?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					

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-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We collect & monitor audit logs and alerts on key events stemming from infrastructure and applications, as well as IAM user and admin activities. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines.		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?	Yes	CSC-owned		Our information security policy covers logging and monitoring. Logs are made available to relevant team members for troubleshooting, auditing, and capacity planning activities. We utilize access control to prevent unauthorized access, deletion, or tampering of logging facilities and log information.		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?	Yes	CSC-owned		Logging includes all relevant events, including all cryptographic operations.		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?	Yes	CSC-owned		Logging includes all relevant events, including all cryptographic operations.		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	CSP-owned		Physical locations logging and monitoring is under the control of our CSP		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?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We collect & monitor audit logs and alerts on key events stemming from infrastructure and applications, as well as IAM user and admin activities. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines. When events and alerts are generated, we correlate those events and alerts across all sources to identify root causes and formally declare incidents, as necessary, in accordance with the Security Incident Response Policy. Additionally, we utilize threat detection solution(s) to actively monitor and alert on network and application-based threats.		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 Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSC-owned		Our information security policy covers logging and monitoring. We use logging solutions and SIEM tools to collect event information. We implements filters, to trigger alerts on logging events that deviate from established system and activity baselines.					
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	CSC-owned		We have a security incident response plan that specifies the scope, security response team, SLAs for incident response, detection and reporting of security incidents, the response procedure and testing of the overall plan		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	
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSC-owned		We have a security incident response plan that specifies the scope, security response team, SLAs for incident response, detection and reporting of security incidents, the response procedure and testing of the overall plan		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	

CAIQ™

GUARDINEX
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
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process		SEF-02		Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
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	CSC-owned		We have a security incident response plan that specifies the scope, security response team, SLAs for incident response, detection and reporting of security incidents, the response procedure and testing of the overall plan		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	CSC-owned		security incident response plan requires that testing of the plan is conducted annually		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	CSC-owned		As soon as the incident has been resolved, the SRT and other relevant team members conduct a post-mortem to better understand the incident that took place, and determine how similar incidents may be prevented in the future. The retrospective should be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner. All incidents are tracked in a ticketing system that can be used to generate reports on the 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	CSC-owned		We have a security incident response plan that specifies the scope, security response team, SLAs for incident response, detection and reporting of security incidents, the response procedure and testing of the overall plan. The response procedure consists of 4 steps: 1. Verification 2. Assessment 3. Containment and mitigation 4. Post-breach response Triaging is done in the Assessment step		SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)		CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSC-owned		We have a security incident response plan that specifies the scope, security response team, SLAs for incident response, detection and reporting of security incidents, the response procedure and testing of the overall plan. The response procedure consists of 4 steps: 1. Verification 2. Assessment 3. Containment and mitigation 4. Post-breach response During the Assessment, If an information security breach has occurred, federal/country-wide law enforcement and local law enforcement should be contacted and informed of the breach. Law enforcement should be contacted in alignment with applicable breach notification laws. Internal and/or external general counsel should lead law enforcement communication efforts (in collaboration with SRT). If general counsel is not available, SRT should lead law enforcement communication efforts. Notification about the information security breach should also be sent to Guardinex customers from whom the breached data subject information is received. The SLA for this notification is 24 hours.		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	CSC-owned		See response to SEF-07.1					
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSC-owned		See response to SEF-07.1		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	CSP-owned		Cloud services provider defines the SSRM		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	CSP-owned		Cloud services provider defines the SSRM					
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned		Cloud services provider defines the SSRM		STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	CSP-owned		Cloud services provider defines the SSRM		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	CSP-owned		Cloud services provider defines the SSRM		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	CSC-owned		The information security policy governs all the controls and procedures that we are responsible for		STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	

GUARDINEX
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-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSC-owned		The information security policy governs all the controls and procedures that we are responsible for		STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	Supply Chain Management, Transparency, and Accountability
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSC-owned		The vendor management policy defines a monitoring process which includes maintaining a list of all vendors and reviewing them periodically		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	CSC-owned		The risk assessment and treatment policy governs our handling of all risks to the organization. We conduct a risk assessment annually.		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	CSC-owned		We have an agreement with our CSP and we also have contracts/agreements with our customers (Guardinex CSCs) that include clauses on scope of services, permitted data use, SLAs, security processes, termination, data privacy, etc		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	CSC-owned		Policies, Agreement Templates are reviewed atleast annually, as part of the Management Review process		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	CSC-owned		Policies, Agreement Templates are reviewed atleast annually, as part of the Management Review process		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	CSC-owned		We have agreements with all our vendors (including supply chain CSPs) that include clauses on information security, confidentiality, data privacy and SLAs		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process		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?	Yes	CSC-owned		We conduct a vendor review annually. This includes all vendors, including supply chain organizations.		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	CSC-owned		We have a vulnerability and patch management policy that mandates: - 3rd party vulnerability assessments periodically - detection and mitigation of vulnerabilities - system/library patching requirements		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					

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	CSC-owned		We have a vulnerability and patch management policy that mandates: - 3rd party vulnerability assessments periodically - detection and mitigation of vulnerabilities - system/library patching requirements We use software on endpoints for threat prevention and monitoring and encrypting storage		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	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
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	CSC-owned		The change management policy defines a specific procedure for Emergency fixes of vulnerabilities. It characterises an emergency and defines the procedure to implement the fix		TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSC-owned		User endpoints are continuously monitored for threats. The Cloud network and infrastructure is also continuously monitored for threats		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	CSC-owned		We have a vulnerability and patch management policy that mandates: - 3rd party vulnerability assessments periodically - detection and mitigation of vulnerabilities - system/library patching requirements		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	CSC-owned		We have a vulnerability and patch management policy that mandates: - 3rd party vulnerability assessments periodically - detection and mitigation of vulnerabilities - system/library patching requirements		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?	Yes	CSC-owned		We have a 3rd party conduct vulnerability assessment / penetration testing annually. In addition, we conduct code scans for security on every change, and application scans for security on every deployment		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	CSC-owned		We rely on the OWASP framework for vulnerability scanning (ZAP)		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?	Yes	CSC-owned		Our security incident response plan includes the policy on stakeholder notification when a vulnerability is identified and it is deemed to be essential for the stakeholders to know (e. g. a vulnerability that could lead to a data breach)		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	CSC-owned		All vulnerabilities identified and remediated are tracked in a ticketing system that can be used to generate reports on the metrics		TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	

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-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSC-owned		We have an endpoint management policy that covers all endpoints used in the organization. The policy specifies the responsiblities of the IT team and Personnel to to ensure the security of company data stored or transmitted on endpoint devices, to prevent unauthorized access to company systems and data, and to ensure compliance with applicable laws and regulations. The policy also specifies the change management process for changes to endpoint devices. The acceptable use policy also specifies requirements for use of endpoints by personnel. Enforcement of the policy is facilitated via software agents that are required to be installed on the endpoints upon provisioning. These software agents protect the endpoint from malware, monitor and enforce controls, and route all network traffic through a gateway that enforces access policies and monitors/reports violations of policy. Some of the endpoint controls are: - password complexity - screen locks, and logouts - use of anti-malware software - use of encryption for data		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	Universal Endpoint Management
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSC-owned		Policies are reviewed atleast annually, as part of the Management Review process					
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	CSC-owned		See response to UEM-01.1		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	CSC-owned		See response to UEM-01.1		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	CSC-owned		The software agents installed on the endpoints report to a central dashboard, and these dashboards provide an inventory of all endpoints in use. This inventory is automatically maintained.		UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
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	CSC-owned		See response to UEM-01.1		UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSC-owned		See response to UEM-01.1		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	CSC-owned		See response to UEM-01.1		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	CSC-owned		Personnel endpoints are required to encrypt storage as per policy, and the encryption status is monitored and enforced through the software agents installed on the endpoints.		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	CSC-owned		Personnel endpoints are required to install the software agents which automatically detect and prevent threats/malware.		UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	

GUARDINEX
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
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSC-owned		Firewalls on endpoint devices are managed and configured via the central dashboard associated with software agents installed		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?	Yes	CSC-owned		DLP measures are implemented through the software agents installed on the device, as well as the network gateway software		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	CSC-owned		Personnel endpoints are required to install the software agents which work with a central device management software to enable policies related to geolocation		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?	Yes	CSC-owned		The configuration and asset management policy defines the process for a lost / stolen endpoint device. End user devices must have encryption enabled, and must have software agents installed. The device encryption status must be monitored and enforced by the IT Security Team. When an asset is reported lost, the IT Security Team must perform a remote wipe of the device when possible.		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	CSC-owned		Third parties that access organizational assets are subject to the endpoint management policy. See response to UEM-01.1 for details.		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