CSA CAIQ

EXOSCALE RESPONSES TO CLOUD SECURITY ALLIANCE CONSENSUS ASSESSMENTS INITIATIVE QUESTIONAIRE

Version 4.0.2

Q2-2022

INTRODUCTION

This document presents Exoscale's responses to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) version 4.0.2

The CAIQ is designed to provide potential consumers of cloud services with information about the security controls in place at a given provider. It is not designed to serve as an exhaustive audit of a provider's security controls, but rather to provide a high-level overview of the provider's security posture.

Exoscale is committed to providing our customers with the highest possible levels of security and privacy, and we believe that the CAIQ is an important tool for helping our customers to understand our security controls. We welcome any questions that our customers may have about our responses to the CAIQ.

Security on public cloud services is a shared responsibility between cloud service providers and cloud service consumers. We have put in place a comprehensive set of security controls to protect our infrastructure and services to ensure that Exoscale meets or exceeds the security expectations of our customers. However, it is the responsibility of our customers to ensure that their applications and data are appropriately secured.

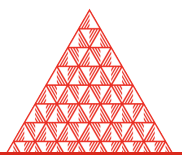
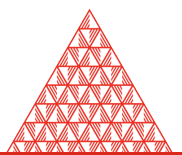


TABLE OF CONTENTS



AUDIT & ASSURANCE

A&A-01 - Audit and Assurance Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale's audit and assurance policies, procedures, and standards are established, documented, approved, communicated, applied, evaluated, and maintained. We have an ISMS that incorporates these policies and procedures, and they are reviewed and updated as necessary. Staff are trained on our policies and procedures, and they are applied during our audits and other assurance activities. Our audit and assurance policies and procedures help us to consistently deliver high-quality audits and other assurance activities. Exoscale's Information Security Management System (ISMS) is updated and reviewed twice a year during the bi-annual security committee. The ISMS is a living document that is updated and adjusted as needed to reflect changes in business needs, risk posture, and regulatory requirements.

Question ID	Question	CSP CAIQ Answer
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes

A&A-02 - Independent Assessments

Control Specifications

Conduct independent audit and assurance assessments according to relevant standards at least annually.

Implementation Description

Exoscale conducts annual audits based on its certification portfolio, which includes

ISO27001/17/18.

Question ID	Question	CSP CAIQ Answer
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes

A&A-03 - Risk Based Planning Assessment

Control Specifications

Perform independent audit and assurance assessments according to risk-based plans and policies.

Implementation Description

Exoscale follows a formal risk assessment methodology that is used to select the appropriate security controls which are audited during our yearly certification cycle. This methodology helps ensure that our independent audit and assurance assessments are performed according to risk-based plans and policies.

Question ID	Question	CSP CAIQ Answer
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes

A&A-04 - Requirements Compliance

Control Specifications

Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.

Implementation Description

Exoscale maintains a list of legal and regulatory requirements as part of its Information Security Management System (ISMS). This list is updated and audited on a yearly basis as part of the certification cycle. Compliance with all relevant standards, regulations, legal/contractual, and statutory requirements is verified as part of the audit.

Question ID	Question	CSP CAIQ Answer
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes

A&A-05 - Audit Management Process

Control Specifications

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.

Implementation Description

Exoscale maintain an audit planning document that defines the activities that needs to be undertaken over the year as part of it's audit and certification cycles. This includes risk assessment, security control assessment, and report reviews. The document is updated and maintained on an ongoing basis to ensure that it accurately reflects the current state of the environment.

Question ID	Question	CSP CAIQ Answer
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes

A&A-06 - Remediation

Control Specifications

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.

Implementation Description

A risk-based corrective action plan is established, documented, approved, communicated, applied, evaluated, and maintained. The plan is documented as part of the risk assessment process, and is communicated to the operational team twice a month. The plan is applied to all audit findings, and is evaluated on a regular basis to ensure that it is effective. The plan is maintained in accordance with the organization's policies and procedures. Audit findings and remediations are communicated with stakeholders during the bi-annual security committee and management reviews. The bi-annual security committee reviews audit findings and remediations and provides a status update to management. Management reviews audit findings and remediations and determines the appropriate course of action.

Question ID	Question	CSP CAIQ Answer
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings	Yes

Question ID	Question	CSP CAIQ Answer
	established, documented, approved, communicated, applied, evaluated, and maintained?	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes

APPLICATION & INTERFACE SECURITY

AIS-01 - Application and Interface Security Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale application and programming interface must be in accordance to the published Exoscale Secure Development Policy which all Exoscale developers must adhere to. All policies part of the Information Security Management System (ISMS) including the Exoscale Secure Development Policy are reviewed twice a year. The reviews include a risk assessment to identify any changes that may need to be made to the policies to ensure they continue to meet the organization's security needs.

Question ID	Question	CSP CAIQ Answer
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes

AIS-02 - Application Security Baseline Requirements

Control Specifications

Establish, document and maintain baseline requirements for securing different applications.

Implementation Description

Exoscale application and programming interface must be in accordance to the published Exoscale Secure Development Policy which all Exoscale developers must adhere to. The policy define general secure development principles, as well as web

application security specific guidelines. In addition, exemples and setup instructions for various software components are available. Baseline for application deployment are defined as part of the automated configuration management platform.

Question ID	Question	CSP CAIQ Answer
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes

AIS-03 - Application Security Metrics

Control Specifications

Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.

Implementation Description

Metrics and KPI are defined and collected for each applications according to business objectives, security requirements and compliance obligation. Operational and technical metrics are collected to measure performance and identify opportunities for improvement.

Question ID	Question	CSP CAIQ Answer
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes

AIS-04 - Secure Application Design and Development

Control Specifications

Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.

Implementation Description

Exoscale follows its defined Architecture Decision Process, which drives its feature development, deployment, and operations. Security requirements are included as part of this process.

Question ID	Question	CSP CAIQ Answer
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes

AIS-05 - Automated Application Security Testing

Control Specifications

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.

Implementation Description

The testing strategy outlines criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals. New systems and versions follow a release process cycle that include automated testing before, during and after the product release. Exoscale make extensive use of automated testing and canaries to ensure application non-regression and security. Exoscale make extensive use of automated testing and canaries to ensure application non-regression and security.

Question ID	Question	CSP CAIQ Answer
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes
AIS-05.2	Is testing automated when applicable and possible?	Yes

AIS-06 - Automated Secure Application Deployment

Control Specifications

Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.

Implementation Description

Exoscale follows the most recent industries best practices in regards to the operation and deployement of its systems. Automated deployement systems are used extensively, including state of the art in-house developped components. Most IT operations are

automated. This includes the deployment and integration of application code. Automation allows for more reliable, consistent, and efficient operations. It also enables faster response to issues and more agile development processes.

Question ID	Question	CSP CAIQ Answer
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes

AIS-07 - Application Vulnerability Remediation

Control Specifications

Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.

Implementation Description

Exoscale follows defined processes for vulnerability management and incident response. Our Vulnerability Management Policy outlines the process for identifying, assessing, and remediating vulnerabilities. Our Incident Response Policy outlines the process for responding to incidents, including identifying and remediating vulnerabilities. Critical security vulnerabilities affecting off-the-shelf components are patched automatically. However, manual remediation is often necessary for vulnerabilities that are not affected by off-the-shelf components.

Question ID	Question	CSP CAIQ Answer
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes

BUSINESS CONTINUITY MANAGEMENT AND OPERATIONAL RESILIENCE

BCR-01 - Business Continuity Management Policy and Procedures

Control Specifications

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.

Implementation Description

A Business Continuity Plan (BCP) and key continuity procedures are documented and reviewed as part of the organization's Information Security Management System (ISMS). The BCP and continuity procedures are also communicated to relevant personnel, and applied as needed. Continuity procedures are also evaluated and maintained as necessary. Exoscale ISMS is updated and reviewed twice a year during the bi-annual security committee. The policy and procedure manual is a living document that is amended and updated as needed.

Question ID	Question	CSP CAIQ Answer
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes

BCR-02 - Risk Assessment and Impact Analysis

Control Specifications

Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.

Implementation Description

The criteria for developing and executing business continuity and operational resilience strategies and capabilities is based on the impacts of business disruptions and risks. The criteria are reviewed twice a year as part of the strategic risk assessment process.

Question ID	Question	CSP CAIQ Answer
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes

BCR-03 - Business Continuity Strategy

Control Specifications

Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.

Implementation Description

Exoscale use a risk vs likelihood risk assessment methodology to assess it's BCR strategies in regards to the effective risk exposure. For example, Exoscale has a Business Continuity Plan (BCP) which is designed to protect its critical business functions in the event of a major incident. The BCP has a number of components, including crisis management, data backup and recovery, and facilities management.

Question ID	Question	CSP CAIQ Answer
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes

BCR-04 - Business Continuity Planning

Control Specifications

Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.

Implementation Description

The organization has a documented business continuity plan that is reviewed and updated regularly. Key continuity procedures have been drafted based on assessed risk exposure, and these procedures are regularly tested and updated as necessary. The organization has also developed a range of operational resilience strategies and capabilities that can be used to maintain business continuity in the event of a disruption. These strategies and capabilities are regularly evaluated and updated as needed.

Question ID	Question	CSP CAIQ Answer
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

BCR-05 - Documentation

Control Specifications

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.

Implementation Description

A documented business continuity plan is in place, and it is updated regularly. Key continuity procedures have been drafted based on assessed risk exposure. Suppliers including datacenter providers are selected based on our security requirements which include resilency to natural and man-made disaster. Relevant documentation is acquired and maintained to support continuity and operational resilience plans. Technical documentation including BCR plans is available on the internal documentation website and is made available to current Exoscale employees. Exoscale ISMS is updated and reviewd twice a year during the bi-annual security commitee. This ensures that the latest updates to the documentation are properly reflected and that all relevant stakeholders are aware of the latest changes.

Question ID	Question	CSP CAIQ Answer
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes

BCR-06 - Business Continuity Exercises

Control Specifications

Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.

Implementation Description

Exoscale conducts and documents the results of multiple continuity drills throughout the year. These drills help ensure that our business continuity and operational resilience plans are effective and can be implemented as needed. We also test our plans when significant changes occur, such as when we launch a new product or service. This helps us ensure that our plans are up-to-date and will continue to meet our needs.

Question ID	Question	CSP CAIQ Answer
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes

BCR-07 - Communication

Control Specifications

Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.

Implementation Description

Exoscale Business Continuity Plan establish communication guidelines to use in the event of a business contintuity event. The plan includes specific steps to take to ensure that key stakeholders and participants are kept apprised of developments and the status of the incident response.

Question ID	Question	CSP CAIQ Answer
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes

BCR-08 - Backup

Control Specifications

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

Implementation Description

Exoscale employs numerous backup strategy for it's systems. Tenants-managed systems's backup are the responsibilty of each respective tenants. The confidentiality, integrity, and availability of backup data is ensured by using state of the art encryption technologies. Off-site backup data is encrypted using the latest encryption technologies to ensure that it is protected from unauthorized access. Backup restoration is part of the regular contintuity drill conducted.

Question ID	Question	CSP CAIQ Answer
BCR-08.1	Is cloud data periodically backed up?	Yes
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes

BCR-09 - Disaster Response Plan

Control Specifications

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.

Implementation Description

A disaster response plan is established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters. The Business Continuity Plan (BCP) outline the crisis-specific response process, responsabilities and communication lines in case of a disaster in order to be able to restore the service as quickly as possible. The BCP is reviewed and updated on a regular basis to ensure that it remains relevant and effective. Exoscale ISMS is updated and reviewed twice a year during the bi-annual security committee. Significant changes are tracked and addressed as necessary.

Question ID	Question	CSP CAIQ Answer
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes

BCR-10 - Response Plan Exercise

Control Specifications

Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.

Implementation Description

Exoscale conducts and documents the results of multiple continuity drills throughout the year. This helps ensure that our team is well-prepared to respond quickly and effectively to any potential incidents. No.

Question ID	Question	CSP CAIQ Answer
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No

BCR-11 - Equipment Redundancy

Control Specifications

Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.

Implementation Description

Exoscale deploys High Availability architectures including redundancy for all it's production system (software, networking and power). In the event of a failure, system redundancy enables automatic failover to a standby system.

Question ID	Question	CSP CAIQ Answer
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

CHANGE CONTROL AND CONFIGURATION MANAGEMENT

CCC-01 - Change Management Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale follows a formal risk management policy to assess strategic and operational risks in regards to its organizationnal assets. This policy is documented, approved, and communicated to all employees. The policy is applied during the asset management process, and any risks identified are evaluated and mitigated as necessary. The policy is maintained and updated as needed. Exoscale ISMS, including its risk management policies and procedures, is updated and reviewed twice a year during the bi-annual security committee.

Question ID	Question	CSP CAIQ Answer
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes

CCC-02 - Quality Testing

Control Specifications

Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.

Implementation Description

Exoscale follows a defined quality change control, approval and testing process. The process includes established baselines, testing, and release standards. Changes to the system must go through a code review process before being merged into the codebase. An automated continuous integration system launches automated tests suites when new code is added to specific software components. Platform updates are first applied and tested on a testing environment before being applied on the production environment using an automated configuration management. Automated monitoring canary script run at planned interval on test and production environment in order to complete end-to-end testing and integration issues.

Question ID	Question	CSP CAIQ Answer
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes

CCC-03 - Change Management Technology

Control Specifications

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).

Implementation Description

Exoscale's asset management policy applies to all organizational assets, regardless of whether they are managed internally or externally. Independent contractors invited to contribute to Exoscale assets must sign the same confidentiality policy as employees and must adhere to the rules and policy defined in Exoscale ISMS.

Question ID	Question	CSP CAIQ Answer
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes

CCC-04 - Unauthorized Change Protection

Control Specifications

Restrict the unauthorized addition, removal, update, and management of organization assets.

Implementation Description

Unauthorized addition, removal, update, and management of organization assets is restricted as stated by our Asset Control Policy as well as the employee employements contractual conditions.

Question ID	Question	CSP CAIQ Answer
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes

CCC-05 - Change Agreements

Control Specifications

Include provisions limiting changes directly impacting CSCs owned environments/ tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.

Implementation Description

Exoscale informs its tenants of changes that are likely to impact them including subprocessors changes as documented in our privacy policy.

Question ID	Question	CSP CAIQ Answer
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	Yes

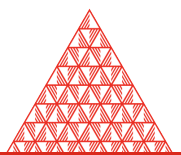
CCC-06 - Change Management Baseline

Control Specifications

Establish change management baselines for all relevant authorized changes on organization assets.

Implementation Description

Change management baselines are established for all relevant authorized changes on organizational assets. Any changes must go through our change management process, which includes getting review and approval of 2 different team members, including security impact considerations. This process helps ensure that all changes are properly authorized, planned, and executed in a controlled manner, minimizing potential disruptions and adverse impacts to the organization.



Question ID	Question	CSP CAIQ Answer
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes

CCC-07 - Detection of Baseline Deviation

Control Specifications

Implement detection measures with proactive notification in case of changes deviating from the established baseline.

Implementation Description

All infrastructure components are deployed against a unified configuration management system. Deviations to the compliance settings in the baseline configuration generate an alert. Dashboard and auditing capabilities of the compliance are available.

Question ID	Question	CSP CAIQ Answer
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes

CCC-08 - Exception Management

Control Specifications

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.

Implementation Description

We use the ITIL change classes and apply different behavior for each of them. Emergency changes result from an incident or outage. Emergency changes do not go through approval, though necessary notification procedures need to be applied. Once normal status is restored, a wrap-up document will be edited to provide feedback on root-cause and actions taken. Exoscale thrive to maintain a set of actionable set of policies and currently has no exemption to its policies. A policy exemption policy defining a process that includes a formal risk assessment and approval at the appropriate level does exists in the event that such an exemption became necessary for operational reasons.

Question ID	Question	CSP CAIQ Answer
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?	Yes

CCC-09 - Change Restoration

Control Specifications

Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.

Implementation Description

Exoscale change process and configuration management tooling allows to quickly roll back changes if it is needed.

Question ID	Question	CSP CAIQ Answer
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

CRYPTOGRAPHY, ENCRYPTION & KEY MANAGEMENT

CEK-01 - Encryption and Key Management Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale maintains a cryptography policy where cryptography, encryption, and key management policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained. This policy is implemented through the use of encryption and key management features within our platform, which are regularly evaluated and updated to ensure their effectiveness. Employees are trained on the use of these features and are required to follow the policy and procedures when accessing or handling data. Exoscale ISMS is updated and reviewed twice a year during the bi-annual security committee.

Question ID	Question	CSP CAIQ Answer
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes

CEK-02 - CEK Roles and Responsibilities

Control Specifications

Define and implement cryptographic, encryption and key management roles and responsibilities.

Implementation Description

Cryptography, encryption, and key management roles and responsibilities are defined and implemented as documented in our asset inventory and cryptography policy. We

use approved cryptography algorithms and protocols to protect our data. Our encryption keys are stored in a secure key management system. Personnel with the appropriate security clearance and authorization have access to the keys on need to have basis.

Question ID	Question	CSP CAIQ Answer
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes

CEK-03 - Data Encryption

Control Specifications

Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.

Implementation Description

Exoscale protects all its endpoints using SSL encryption to protect in-transit traffic. At the moment, data at-rest in not encrypted by Exoscale.

Question ID	Question	CSP CAIQ Answer
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes

CEK-04 - Encryption Algorithm

Control Specifications

Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.

Implementation Description

The Cryptography Policy defines a list of approved cryptographic algorithms that can be used to protect data. The policy considers data classification, associated risks, and encryption technology usability when selecting an appropriate algorithm.

Question ID	Question	CSP CAIQ Answer
CEK-04.1	Are appropriate data protection encryption algorithms used that consider	Yes

Question ID	Question	CSP CAIQ Answer
	data classification, associated risks, and encryption technology usability?	

CEK-05 - Encryption Change Management

Control Specifications

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.

Implementation Description

Standard change management procedures are in place to review, approve, and communicate changes to cryptography, encryption, and key management technology. Any changes that are made to accommodate internal and external sources must go through this process. This ensures that all changes are made in a safe and secure manner, and that any potential impacts are accounted for.

Question ID	Question	CSP CAIQ Answer
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes

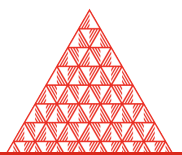
CEK-06 - Encryption Change Cost Benefit Analysis

Control Specifications

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.

Implementation Description

Any changes to cryptography, encryption and key management-related systems, policies, and procedures are managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. This is done as part of the regular change management process, which includes a security impact assessment.



Question ID	Question	CSP CAIQ Answer
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes

CEK-07 - Encryption Risk Management

Control Specifications

Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.

Implementation Description

A cryptography, encryption, and key management risk program is established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions. The risk program is an integral part of the overall product development process, and cryptography, encryption, and key management changes go through the formal product development process that includes risk management and monitoring.

Question ID	Question	CSP CAIQ Answer
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes

CEK-08 - CSC Key Management Capability

Control Specifications

CSPs must provide the capability for CSCs to manage their own data encryption keys.

Implementation Description

Most CSPs do not provide their customers with the ability to manage their own encryption keys. This means that the CSC is responsible for encrypting and decrypting data as it moves in and out of the cloud, and the CSP has no visibility into the data. In some cases, the CSP will manage the encryption keys on behalf of the customer, but they will not have access to them.

Question ID	Question	CSP CAIQ Answer
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No

CEK-09 - Encryption and Key Management Audit

Control Specifications

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).

Implementation Description

Exoscale does not have a specific frequency for auditing encryption and key management systems, policies, and processes. However, the Exoscale Cryptography Policy is reviewed twice a year. The cryptography policy can however be changed at any time depending on security events. Encryption and key management systems, policies, and processes are audited (preferably continuously but at least annually).

Question ID	Question	CSP CAIQ Answer
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?	No
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes

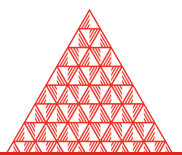
CEK-10 - Key Generation

Control Specifications

Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.

Implementation Description

Exoscale uses Hashicorp Vault to manage and maintain his cryptographic keys. Vault uses a deterministic random number generator (DRNG) to generate cryptographic keys. The Vault PRNG is cryptographically secure and has been tested against known attacks.



Question ID	Question	CSP CAIQ Answer
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes

CEK-11 - Key Purpose

Control Specifications

Manage cryptographic secret and private keys that are provisioned for a unique purpose.

Implementation Description

Exoscale uses Hashicorp Vault to manage and maintain his cryptographic keys and tries to increasingly use short-lived, frequently cycled keys.

Question ID	Question	CSP CAIQ Answer
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes

CEK-12 - Key Rotation

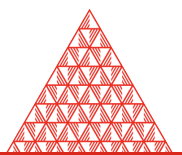
Control Specifications

Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.

Implementation Description

Exoscale is using key management automation to cycle keys and certificate with a high frequency. This assures that keys are rotated frequently enough to mitigate the risk of information disclosure, while also taking into account any legal or regulatory requirements.

Question ID	Question	CSP CAIQ Answer
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes



CEK-13 - Key Revocation

Control Specifications

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.

Implementation Description

Exoscale uses a certificate revocation list (CRL) to revoke certificates that are no longer part of the organization. The CRL is a list of revoked certificates that is published by the certificate authority (CA) that issued the certificates. When a certificate is revoked, the CA updates the CRL and sends it to all of the organizations that have subscribed to the CRL.

Question ID	Question	CSP CAIQ Answer
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes

CEK-14 - Key Destruction

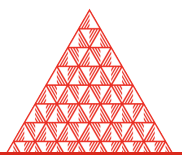
Control Specifications

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.

Implementation Description

Certificate revocation lists (CRLs) and certificate Revocation Requests (CRRs) are used to revoke certificates. Key escrow and recovery processes are in place in the event that the key is needed to recover data. Key destruction processes are in place to destroy keys when they are no longer needed.

Question ID	Question	CSP CAIQ Answer
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes



CEK-15 - Key Activation

Control Specifications

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.

Implementation Description

Exoscale keys are managed according to our published cryptography policy and have comprehensive documented procedures for its PKI infrastructure management. The generation and activation of keys are based on a defined schedule and are only performed by authorized personnel. Key rotation is also performed on a regular basis in accordance with our cryptography policy.

Question ID	Question	CSP CAIQ Answer
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

CEK-16 - Key Suspension

Control Specifications

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.

Implementation Description

Exoscale keys are managed according to our published cryptography policy and have comprehensive documented procedures for its PKI infrastructure management. These processes, procedures, and technical measures are designed to monitor, review and approve key transitions, including legal and regulatory requirement provisions. The effectiveness of these processes, procedures, and technical measures are evaluated on a regular basis.

Question ID	Question	CSP CAIQ Answer
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

CEK-17 - Key Deactivation

Control Specifications

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.

Implementation Description

Exoscale has a published cryptography policy that governs the management of keys. This policy includes comprehensive documented procedures for its PKI infrastructure management. These procedures include provisions for deactivating keys at the time of their expiration date. Key deactivation processes are routinely evaluated to ensure they meet all legal and regulatory requirements.

Question ID	Question	CSP CAIQ Answer
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

CEK-18 - Key Archival

Control Specifications

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.

Implementation Description

All cryptographic keys are stored in a secure repository. The repository need to be cryptographically unsealed by multiple person to allow access to the root keys controlling the Exoscale PKI infrastructure.

Question ID	Question	CSP CAIQ Answer
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

CEK-19 - Key Compromise

Control Specifications

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.

Implementation Description

Exoscale has a formal information classification policy that defines handling rules for various class of data, including when the data is required to be stored securely and whether it should be encrypted. The policy is based on applicable legal and regulatory requirements. Procedures and technical measures to encrypt information are implemented in accordance with the policy. These procedures and measures are evaluated to ensure they meet the required standard.

Question ID	Question	CSP CAIQ Answer
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes

CEK-20 - Key Recovery

Control Specifications

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.

Implementation Description

Exoscale has implemented a formal risk assessment process including operational continuity risks related to the use of cryptography. This process includes the identification of risks, the assessment of the likelihood and impact of those risks, and the development of mitigation strategies. Exoscale also conducts periodic reviews of its risk assessment process to ensure that it continues to meet the organization's needs.

Question ID	Question	CSP CAIQ Answer
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and	Yes

Question ID	Question	CSP CAIQ Answer
	exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	

CEK-21 - Key Inventory Management

Control Specifications

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.

Implementation Description

Exoscale keys are managed according to our published cryptography policy and have comprehensive documented procedures for its PKI infrastructure management. Legal and regulatory requirements in our operating jurisdiction in regards to cryptography are taken into account when reviewing the cryptography policy. Procedures for the management of cryptographic keys are implemented and evaluated on a regular basis to ensure compliance with legal and regulatory requirements.

Question ID	Question	CSP CAIQ Answer
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

DATACENTER SECURITY

DCS-01 - Off-Site Equipment Disposal Policy and Procedures

Control Specifications

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.

Implementation Description

Policies and procedures for the secure disposal of equipment used outside the organization's premises are documented in the employee confidentiality policy and the asset management procedures (disponal of assets). The employee confidentiality policy requires employees to return all equipment and materials used in the course of their work to the organization's premises. The asset management procedures require employees to follow certain procedures for the disposal of equipment, including the secure disposal of equipment used outside the organization's premises. Data destruction procedures are in place that render information recovery impossible if equipment is not physically destroyed. Media disposal follows the documented secure disposal of media policy. Exoscale ISMS is updated and reviewd twice a year during the bi-annual security commitee.

Question ID	Question	CSP CAIQ Answer
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes

DCS-02 - Off-Site Transfer Authorization Policy and Procedures

Control Specifications

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.

Implementation Description

A policy for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location is established, documented, approved, communicated, implemented, enforced, and maintained. The Off-Site Transfer Policy defines the rules governing the transfer of hardware and data between alternate locations. This policy states that no data is ever-physically transferred and that hardware must be wiped according to our data disposal policy before being transferred from site to site. Any transfer of hardware from an Exoscale site to another requires a signed shipping manifest. This manifest must include the cryptographic verification of the authorization to transfer the hardware. Exoscale ISMS is updated and reviewd twice a year during the bi-annual security commitee.

Question ID	Question	CSP CAIQ Answer
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes

DCS-03 - Secure Area Policy and Procedures

Control Specifications

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.

Implementation Description

No specific policies have been documented, but general health and safety regulations and guidelines are followed. Employee working hours are regulated by the Swiss labor law, and health and safety guidelines are communicated to employees. Health and

safety inspections are conducted regularly, and safety violations are corrected promptly. Exoscale HR department work to maintain a safe, secure working environment for its employees in line with Swiss working regulations. However, specific policies and procedures for maintaining safe, secure working environments are not reviewed and updated at least annually.

Question ID	Question	CSP CAIQ Answer
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?	No
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	No

DCS-04 - Secure Media Transportation Policy and Procedures

Control Specifications

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.

Implementation Description

Our policies and procedures for the secure transportation of physical media are established, documented, approved, communicated, enforced, evaluated, and maintained. Off-site transportation of physical media is not permited by our current policies. Exoscale ISMS is updated and reviewd twice a year during the bi-annual security commitee.

Question ID	Question	CSP CAIQ Answer
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes

DCS-05 - Assets Classification

Control Specifications

Classify and document the physical, and logical assets (e.g., applications) based on the

organizational business risk.

Implementation Description

The classification and documentation of physical and logical assets is based on the organizational business risk. All assets are classified according to their business value and the risk that affect them. This allows the organization to focus on the most important assets and protect them from potential threats.

Question ID	Question	CSP CAIQ Answer
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes

DCS-06 - Assets Cataloguing and Tracking

Control Specifications

Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.

Implementation Description

All logical access to the infrastructure are logged for 1 year. Physical access and hardware intervention request to smart-hands services are logged and tracked.

Question ID	Question	CSP CAIQ Answer
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes

DCS-07 - Controlled Access Points

Control Specifications

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.

Implementation Description

Exoscale hosts its services from datacenters matching its datacenter requirements which include state of the art physical security. The HQ office does not contain any infrastructure nor customer data and is secured at the appropriate level for office space use (secure lock, video surveillance). All Exoscale infrastructure is hosted in state of the art data centers operated by well-known datacenter operators (Equinix, A1 group). These data centers are built with multiple layers of physical security, including perimeter

fencing, biometric access controls, video surveillance, and 24x7 security staff.

Question ID	Question	CSP CAIQ Answer
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes

DCS-08 - Equipment Identification

Control Specifications

Use equipment identification as a method for connection authentication.

Implementation Description

Authentication through connection equipment identification is used in some cases. One example of this is the use of hardware cryptographic tokens. These tokens are used to generate a unique code that is matched against a code stored on the authentication server. This code is used to verify the identity of the user attempting to connect to the network.

Question ID	Question	CSP CAIQ Answer
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes

DCS-09 - Secure Area Authorization

Control Specifications

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.

Implementation Description

Access to secure areas is restricted to authorized personnel only. Ingress and egress areas are documented and monitored by physical access control mechanisms. Employees with physical access to the infrastructure are well documented and limited on a need to have basis. Bi-weekly access control reviews are conducted to ensure that access logs are kept up to date. Access logs are kept for one year.

Question ID	Question	CSP CAIQ Answer
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes

DCS-10 - Surveillance System

Control Specifications

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.

Implementation Description

Exoscale datacenters operators implements surveillance systems and protocols around their external perimeter at all ingress and egress points. This includes, but is not limited to, closed-circuit television (CCTV), intrusion detection systems (IDS), and access control lists (ACLs).

Question ID	Question	CSP CAIQ Answer
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes

DCS-11 - Unauthorized Access Response Training

Control Specifications

Train datacenter personnel to respond to unauthorized ingress or egress attempts.

Implementation Description

Exoscale datacenters operators are trained to respond to unauthorized access or egress attempts.

Question ID	Question	CSP CAIQ Answer
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes

DCS-12 - Cabling Security

Control Specifications

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.

Implementation Description

The company has a defined process for risk-based protection of power and telecommunication cables from interception, interference, or damage threats. Procedures are in place to ensure that these processes are implemented and evaluated. Technical measures are also in place to protect cables from damage. These measures are reviewed and updated as necessary.

Question ID	Question	CSP CAIQ Answer
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

DCS-13 - Environmental Systems

Control Specifications

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.

Implementation Description

Our environmental control systems are designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards. Our operators are held to a Service Level Agreement (SLA) that guarantees these conditions will be met, and we regularly audit our systems to ensure compliance.

Question ID	Question	CSP CAIQ Answer
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes

DCS-14 - Secure Utilities

Control Specifications

Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.

Implementation Description

Utility services are secured, monitored, maintained, and tested at planned intervals for continual effectiveness. Datacenter operators conduct regular tests of their power redundancy protocols and hardware. This helps ensure that the systems are always up and running, and that any issues are identified and addressed quickly.

Question ID	Question	CSP CAIQ Answer
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes

DCS-15 - Equipment Location

Control Specifications

Keep business-critical equipment away from locations subject to high probability for environmental risk events.

Implementation Description

Business-critical equipment is segregated from locations that are subject to a high probability of environmental risk events. Datacenters are selected after a risk-based assessment that disqualifies locations that are subject to a high probability of environmental risk events.

Question ID	Question	CSP CAIQ Answer
DCS-15.1	Is business-critical equipment segregated from locations subject to a	Yes

Question ID	Question	CSP CAIQ Answer
	high probability of environmental risk events?	

DATA SECURITY AND PRIVACY LIFECYCLE MANAGEMENT

DSP-01 - Security and Privacy Policy and Procedures

Control Specifications

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.

Implementation Description

Our policies and procedures are 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. Data is labelled and classified according to our Information Classification policy. Marking, reproduction, distribution and disposal requirements are defined for each defined class. Exoscale ISMS is updated and reviewd twice a year during the bi-annual security commitee.

Question ID	Question	CSP CAIQ Answer
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes

DSP-02 - Secure Disposal

Control Specifications

Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.

Implementation Description

The asset disposal procedure ensure that data is properly disposed of when

decomissioning media support. The process includes degaussing or overwriting of the data media with a secure erase algorithm.

Question ID	Question	CSP CAIQ Answer
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

DSP-03 - Data Inventory

Control Specifications

Create and maintain a data inventory, at least for any sensitive data and personal data.

Implementation Description

A data inventory is created and maintained for sensitive and personal information. The information assets are listed in our asset inventory, which is used to track and manage our information resources. This helps us ensure that our sensitive and personal information is properly protected.

Question ID	Question	CSP CAIQ Answer
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes

DSP-04 - Data Classification

Control Specifications

Classify data according to its type and sensitivity level.

Implementation Description

Our organization classifies all information assets according to their level of sensitivity. This helps us to ensure that only authorized individuals have access to the most sensitive data. We also use this classification system to help us determine the appropriate security measures that need to be in place to protect the data.

Question ID	Question	CSP CAIQ Answer
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes

DSP-05 - Data Flow Documentation

Control Specifications

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.

Implementation Description

Data flows of personal data are tracked in the registry of processing activities. The registry is a tool used to identify and manage risks associated with the processing of personal data. The registry is updated with information on the type of data processed, the purpose of the processing, the recipients of the data, and the location of the data. Data privacy policies and documentation is reviewed yearly. This is to ensure that all data is processed in a way that is compliant with the organization's data privacy policies. Additionally, changes to the data flow (e.g. new applications or changes to the way data is processed) will trigger a review of the data privacy policies and documentation.

Question ID	Question	CSP CAIQ Answer
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes

DSP-06 - Data Ownership and Stewardship

Control Specifications

Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.

Implementation Description

The ownership of sensitive data is documented in the asset inventory. This includes the name of the individual or organization who owns the data, as well as contact information for the owner. In addition, the responsible party for managing and safeguarding the data is identified. The asset inventory documentation is reviewed twice a year.

Question ID	Question	CSP CAIQ Answer
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes
DSP-06.2	Is data ownership and stewardship documentation reviewed at least	Yes

Question ID	Question	CSP CAIQ Answer
	annually?	

DSP-07 - Data Protection by Design and Default

Control Specifications

Develop systems, products, and business practices based upon a principle of security by design and industry best practices.

Implementation Description

Exoscale follows a secure development policy that ensures that systems, products, and business practices are based on security principles by design and per industry best practices. This policy helps to ensure that our products are secure and meet the expectations of our customers.

Question ID	Question	CSP CAIQ Answer
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes

DSP-08 - Data Privacy by Design and Default

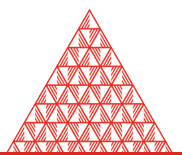
Control Specifications

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.

Implementation Description

Exoscale follows the group data privacy policy and its principles. Exoscale follows the group data privacy policy and its principles. The group data privacy policy is a set of rules that ensure that all Exoscale users' data is treated in a way that complies with all applicable laws and regulations.

Question ID	Question	CSP CAIQ Answer
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes



Question ID	Question	CSP CAIQ Answer
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes

DSP-09 - Data Protection Impact Assessment

Control Specifications

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.

Implementation Description

DPIA's are conducted when new subprocessors are introduced, as well as when there is a change in the processing purpose, or when there is a change in the personal data that is processed. The DPIA helps identify and mitigate any risks associated with the processing of personal data.

Question ID	Question	CSP CAIQ Answer
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

DSP-10 - Sensitive Data Transfer

Control Specifications

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.

Implementation Description

The asset classification policy defines the requirements for the transfer of personal or sensitive data. Procedures are in place to ensure that only authorized personnel are able to access the data, and that it is only processed in accordance with the applicable laws and regulations. Technical measures are in place to protect the data from unauthorized access.

Question ID	Question	CSP CAIQ Answer
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes

DSP-11 - Personal Data Access, Reversal, Rectification and Deletion

Control Specifications

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.

Implementation Description

Exoscale follows EU-GDPR and Swiss data privacy laws and has documented and implemented all the required procedures in its Exoscale Data Privacy Handbook. The Handbook covers the right of data subjects to access their data, request modifications, and delete their data. It also includes the technical and organizational measures that Exoscale has put in place to protect data subjects' personal data.

Question ID	Question	CSP CAIQ Answer
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

DSP-12 - Limitation of Purpose in Personal Data Processing

Control Specifications

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.

Implementation Description

Exoscale follows the EU-GDPR and Swiss data privacy laws and has implemented all the required procedures in its Exoscale Data Privacy Handbook. This handbook defines the processes and technical measures that are used to ensure that personal data is processed in accordance with the applicable laws and regulations. It also specifies the purposes for which the data is being processed and provides the necessary information to the data subjects about their rights.

Question ID	Question	CSP CAIQ Answer
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

DSP-13 - Personal Data Sub-processing

Control Specifications

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.

Implementation Description

Exoscale follows EU-GDPR and Swiss data privacy laws and has documented and implemented processes, procedures and technical measures in the event that sub-processing of client data takes place. Currently the only case where such sub-processing takes place is through our DBaaS service. In order to provide our DBaaS service, Exoscale partners with a third-party provider who has been assesed to comply to EU-GDPR and Swiss data privacy laws.

Question ID	Question	CSP CAIQ Answer
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

DSP-14 - Disclosure of Data Sub-processors

Control Specifications

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.

Implementation Description

Our use of sub-processors is documented on our privacy policy page, which is available to our customers. We also list the services that require the use of sub-processors, such as our DBaaS offering. Customers can decide not to use such services if they do not want their personal or sensitive data to be accessed by sub-processors. In the event of the addition of a new sub-processor on an existing service, tenants will be notified 30 days in advance.

Question ID	Question	CSP CAIQ Answer
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

DSP-15 - Limitation of Production Data Use

Control Specifications

Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.

Implementation Description

Our organization does not allow the replication or use of production data in non-production environments. We have policies in place that govern the use of data, and the associated risks are managed by ensuring that only authorized users have access to data. We also have controls in place to monitor and track data usage. By limiting access to data and monitoring its use, we are able to reduce the risk of data misuse or unauthorized access.

Question ID	Question	CSP CAIQ Answer
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	NA

DSP-16 - Data Retention and Deletion

Control Specifications

Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.

Implementation Description

Exoscale follows business requirements, applicable laws, and regulations when it comes to data retention, archiving, and deletion practices. Exoscale has a list of its legal, regulatory and contractual requirements, and ensures that its data retention, archiving and deletion practices follow those requirements.

Question ID	Question	CSP CAIQ Answer
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes

DSP-17 - Sensitive Data Protection

Control Specifications

Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.

Implementation Description

Sensitive data is protected through a variety of means, including but not limited to physical security, access controls, and data encryption. Information assets are inventoried and classified according to our Information Classification rules which define appropriate handling rules.

Question ID	Question	CSP CAIQ Answer
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes

DSP-18 - Disclosure Notification

Control Specifications

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.

Implementation Description

Exoscale has a documented handling procedure for disclosure request by Law Enforcement Agency. The procedure is designed to ensure that only lawful requests by Swiss authorities are considered and that affected customers are notified unless prevented to do so by law. Exoscale has a documented handling procedure for disclosure request by Law Enforcement Agency. Only lawful requests by Swiss authorities are considered and affected customers are notified unless prevented to do so by law.

Question ID	Question	CSP CAIQ Answer
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes

DSP-19 - Data Location

Control Specifications

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.

Implementation Description

Exoscale does not transfer its client data outside of the CSC selected location. The locations of eventual suprocessing are listed in our privacy page.

Question ID	Question	CSP CAIQ Answer
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

GOVERNANCE, RISK AND COMPLIANCE

GRC-01 - Governance Program Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale top management team recognize (based on tenants claims) that information security should be managed in compliance with the most stringent industry standards and it was decided that Exoscale implement an Information Security Management System (ISMS) with the goal of maintaining a track record of excellence in terms of information security. This includes the policies and procedures that are necessary to support the governance of information. These policies and procedures are documented, approved, communicated, applied, evaluated, and maintained. Policies and precedures are reviewed and updated twice a year by the Exoscale security commitee during our bi-annual ISMS review.

Question ID	Question	CSP CAIQ Answer
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes

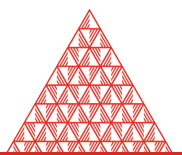
GRC-02 - Risk Management Program

Control Specifications

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.

Implementation Description

Exoscale has implemented a Risk Assessment and Risk treatment methodology based



the Wise Security Risk Assessment framework as published at https://wiki.geant.org/display/WISE/RAW-WG. This methodology is documented in the Exoscale Security documentation and is regularly reviewed and updated.

Question ID	Question	CSP CAIQ Answer
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes

GRC-03 - Organizational Policy Reviews

Control Specifications

Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.

Implementation Description

Policies and procedures are reviewed and updated twice a year by the Exoscale security committee during our bi-annual ISMS review.

Question ID	Question	CSP CAIQ Answer
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes

GRC-04 - Policy Exception Process

Control Specifications

Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.

Implementation Description

An approved exception process is mandated by the governance program established and followed whenever a deviation from an established policy occurs. Exoscale's set of actionable policies is maintained and any deviation from these policies must be justified and approved through the established exception process. This process includes a formal risk assessment and approval at the appropriate level.

Question ID	Question	CSP CAIQ Answer
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes

GRC-05 - Information Security Program

Control Specifications

Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.

Implementation Description

Exoscale has implemented and run an ISO27001-certified ISMS program since 2018. The program covers all relevant CCM domains, including risk management, asset management, security incident management, and communication and training. Exoscale's ISMS has been certified by an accredited third-party auditor.

Question ID	Question	CSP CAIQ Answer
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes

GRC-06 - Governance Responsibility Model

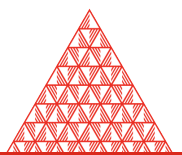
Control Specifications

Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.

Implementation Description

Roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs are defined and documented in our Information Security Policy. This policy is available to all employees and is regularly reviewed and updated as needed.

Question ID	Question	CSP CAIQ Answer
GRC-06.1	Are roles and responsibilities for planning, implementing, operating,	Yes



Question ID	Question	CSP CAIQ Answer
	assessing, and improving governance programs defined and documented?	

GRC-07 - Information System Regulatory Mapping

Control Specifications

Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.

Implementation Description

Exoscale maintains a list of its legal, regulatory and contractual requirements as part of its ISMS. This list is reviewed and updated as necessary to ensure that all relevant standards, regulations, legal/contractual, and statutory requirements are identified and documented.

Question ID	Question	CSP CAIQ Answer
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes

GRC-08 - Special Interest Groups

Control Specifications

Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.

Implementation Description

Exoscale maintain membership or contact with a number of cloud-related organizations and interest groups, including the Cloud Native Computing Foundation (CNCF) and Cloud Security Alliance (CSA). We also collaborate with other members of the community to develop best practices and standards for cloud computing.

Question ID	Question	CSP CAIQ Answer
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes

HUMAN RESOURCES

HRS-01 - Background Screening Policy and Procedures

Control Specifications

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.

Implementation Description

New team members including employees and contractors are subject to a mandatory background check as part of the onboarding process. The company has a policy for conducting background checks, which is documented and approved. The policy is communicated to new employees and contractors, and the background check process is applied to all new hires. The company evaluates the effectiveness of its background check policy on an ongoing basis. Background verification policies and procedures are designed to meet the specific needs of the company and the regulations of the area in which they operate. They are also designed to protect the privacy of the employees and to protect the company from potential liability. The background check procedure is reviewed yearly.

Question ID	Question	CSP CAIQ Answer
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes

HRS-02 - Acceptable Use of Technology Policy and Procedures

Control Specifications

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.

Implementation Description

Acceptable use of organization resources is documented in the employee confidentiality policy. This policy outlines the specific conditions and allowances for the acceptable use of organizationally-owned or managed assets. The policy is communicated to all employees, and is applied and evaluated on a regular basis. The acceptable use of organization resources is documented in the employee confidentiality policy. The employee confidentiality policy is reviewed yearly and any updates to the acceptable use of resources are incorporated into the policy.

Question ID	Question	CSP CAIQ Answer
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes

HRS-03 - Clean Desk Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has a clean desk policy that employees accept by signing the employee confidentiality agreement. This policy requires that all confidential data be concealed when the workspace is left unattended. Employees are also required to keep their computers locked when they are not in use. The clean-desk policy is documented in the employee confidentiality policy which is reviewed yearly.

Question ID	Question	CSP CAIQ Answer
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes

HRS-04 - Remote and Home Working Policy and Procedures

Control Specifications

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.

Implementation Description

Remote-work policies and procedures are documented in the employee confidentiality policy. This policy is approved by the management team and communicated to all employees. Employees are trained on the policy and are required to sign a confidentiality agreement. Procedures for accessing, processing, and storing information at remote sites are established and followed. These procedures are evaluated and updated as needed. The employee confidentiality policy is reviewed anually. In addition, any policies and procedures related to the protection of information accessed, processed, or stored at remote sites and locations are also reviewed and updated at least annually.

Question ID	Question	CSP CAIQ Answer
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes

HRS-05 - Asset returns

Control Specifications

Establish and document procedures for the return of organization-owned assets by terminated employees.

Implementation Description

The return of assets policy, procedures, and checklist are documented and reviewed annually.

Question ID	Question	CSP CAIQ Answer
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes

HRS-06 - Employment Termination

Control Specifications

Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.

Implementation Description

Exoscale Employees confidentiality policy documents the roles and responsabilities of its employees including during changes in employements (hire, transfer, termination). This policy is communicated to all personnel and is available to all employees.

Question ID	Question	CSP CAIQ Answer
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	

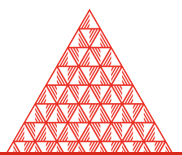
HRS-07 - Employment Agreement Process

Control Specifications

Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.

Implementation Description

In order to protect company information, systems, resources, and assets, employees and contractors must sign a work contract in addition to the employee confidentiality policy. This contract outlines the expectations and responsibilities of the employee or contractor in regards to protecting company information. This includes agreeing to not disclose any confidential information, to follow all security protocols, and to comply with all company policies and procedures.



Question ID	Question	CSP CAIQ Answer
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes

HRS-08 - Employment Agreement Content

Control Specifications

The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.

Implementation Description

Provisions and/or terms for adherence to established information governance and security policies are typically included in employment agreements. For example, the employee confidentiality policies may include terms requiring the employee to comply with the organization's information security and data privacy policies.

Question ID	Question	CSP CAIQ Answer
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes

HRS-09 - Personnel Roles and Responsibilities

Control Specifications

Document and communicate roles and responsibilities of employees, as they relate to information assets and security.

Implementation Description

Employees roles and responsabilities are documented in the Exoscale Information Security Policy. The policy defines the specific roles and responsibilities of employees with respect to information security. Employees are required to comply with the policy and are held accountable for their actions with respect to information security.

Question ID	Question	CSP CAIQ Answer
HRS-09.1	Are employee roles and responsibilities relating to information assets	Yes

Question ID	Question	CSP CAIQ Answer
	and security documented and communicated?	

HRS-10 - Non-Disclosure Agreements

Control Specifications

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.

Implementation Description

The employee confidentiality policies includes terms pertaining to non-disclosure of confidential and internal informations. This is done to protect the organization's data protection needs and operational details. The requirements for non-disclosure/ confidentiality agreements are reviewed at planned intervals to ensure that they continue to reflect the organization's data protection needs and operational details.

Question ID	Question	CSP CAIQ Answer
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes

HRS-11 - Security Awareness Training

Control Specifications

Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.

Implementation Description

The organization conducts regular awareness training exercises on an annual basis. The training is aimed at all employees, and covers a variety of security-related topics. The training is documented and approved by management, and communicated to all employees. It is applied in a consistent fashion, and is evaluated and maintained on an ongoing basis. Regular security awareness training updates are provided. A new training module is typically released each year, and all employees are required to complete the training annually.

Question ID	Question	CSP CAIQ Answer
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes
HRS-11.2	Are regular security awareness training updates provided?	Yes

HRS-12 - Personal and Sensitive Data Awareness and Training

Control Specifications

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.

Implementation Description

All employees and contractors are granted access to sensitive organizational and personal data, provided they have received the appropriate security awareness training. Security awareness training covers topics such as how to protect sensitive data, how to identify and report suspicious activity, and how to comply with the organization's security policies. All employees are granted access to sensitive organizational and personal data. The company publishes policies and procedures related to employee professional function on the company wide internal documentation. This allows employees to access and reference the most up to date information related to their role in the company.

Question ID	Question	CSP CAIQ Answer
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes

HRS-13 - Compliance User Responsibility

Control Specifications

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.

Implementation Description

Compliance training are part of the regular training schedule. Employees are provided with an overview of the company's compliance policies and procedures, as well as their specific roles and responsibilities in relation to compliance. Employees are also kept up-to-date on any changes to the compliance policies and procedures, as well as any new legal, statutory, or regulatory compliance obligations that may apply to the company.

Question ID	Question	CSP CAIQ Answer
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

IDENTITY & ACCESS MANAGEMENT

IAM-01 - Identity and Access Management Policy and Procedures

Control Specifications

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.

Implementation Description

Identity and access management policies and procedures are established, documented, approved, communicated, implemented, applied, evaluated, and maintained as part of the company's Access Control Policy. The identity and access management policies and procedures are designed to ensure that only authorized users are able to access the company's information systems and data. The identity and access management policies and procedures are reviewed and updated as necessary to ensure that they continue to meet the company's needs. The access control policy is reviewed yearly. Additionally, the identity and access management procedures are reviewed and updated at least annually.

Question ID	Question	CSP CAIQ Answer
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes

IAM-02 - Strong Password Policy and Procedures

Control Specifications

Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.

Implementation Description

Exoscale's password policies mandate that passwords should follow the NIST 800 63-b

published guidelines. Our password policies are communicated to all employees, and our procedures for implementing and enforcing these policies are outlined in our IT Security Policy. We regularly evaluate our password policies and procedures to ensure that they are effective in protecting our data. The password policy is reviewed as part of the access control policy review, which is conducted at least annually.

Question ID	Question	CSP CAIQ Answer
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes

IAM-03 - Identity Inventory

Control Specifications

Manage, store, and review the information of system identities, and level of access.

Implementation Description

System identity information and levels of access are managed, stored, and reviewed. Access rights and levels are reviewed twice a month.

Question ID	Question	CSP CAIQ Answer
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes

IAM-04 - Separation of Duties

Control Specifications

Employ the separation of duties principle when implementing information system access.

Implementation Description

The separation of duties principle is employed when implementing information system access. This is done in order to minimize the risk of unauthorized access, alteration, or destruction of data. Exoscale strives to implement segregation of duties principles as much as possible in order to protect our customers' data.

Question ID	Question	CSP CAIQ Answer
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes

IAM-05 - Least Privilege

Control Specifications

Employ the least privilege principle when implementing information system access.

Implementation Description

The least privilege principle is employed when implementing information system access. Access to information and system are restricted based on least priviledge principles. This means that users are only given access to the information and system they need to do their job and no more. This helps to protect the information and system from unauthorized access and misuse.

Question ID	Question	CSP CAIQ Answer
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes

IAM-06 - User Access Provisioning

Control Specifications

Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.

Implementation Description

User access procedures are described in the access control policies. Users access right are documented and regularly reviewed.

Question ID	Question	CSP CAIQ Answer
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes

IAM-07 - User Access Changes and Revocation

Control Specifications

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.

Implementation Description

User deregistration procedures are documented and are triggered immediately upon an employee or contractor leaving. Upon termination, access is immediately revoked and the user is removed from all systems. Additionally, upon a system-level identity change (e.g., a change in role, department, or manager), the relevant accesses are reviewed and updated as necessary.

Question ID	Question	CSP CAIQ Answer
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes

IAM-08 - User Access Review

Control Specifications

Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.

Implementation Description

Access reviews and access control policy reviews are completed with a frequency commensurate with organizational risk tolerance. Access reviews are conducted twice a month and access control policies are reviewed twice a year as part of the ISMS review.

Question ID	Question	CSP CAIQ Answer
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes

IAM-09 - Segregation of Privileged Access Roles

Control Specifications

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.

Implementation Description

Processes, procedures, and technical measures for the segregation of privileged access roles are defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate. Encryption, key management capabilities, and logging capabilities are restricted to an identified subset of the operations team.

Question ID	Question	CSP CAIQ Answer
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes

IAM-10 - Management of Privileged Access Roles

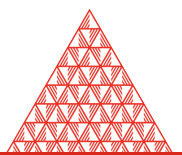
Control Specifications

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.

Implementation Description

An access process is defined and implemented to ensure privileged access roles and rights are granted for a limited period. Access are granted based on specific employee or contractor role and responsabilites. Upon role or responsability changes, access right are reviewed and changed to match the new role and responsabilities. Exoscale periodically reviews the privileged access permissions of its employees to ensure that they are appropriate for their current role and responsibilities. Employees are only granted privileged access if it is absolutely necessary for them to perform their job duties. In addition, employees are regularly reminded of the importance of safeguarding privileged access credentials and are required to comply with strict security policies and procedures.

Question ID	Question	CSP CAIQ Answer
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	No



IAM-11 - CSCs Approval for Agreed Privileged Access Roles

Control Specifications

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.

Implementation Description

The process for granting access for high-risk privileged access roles is defined, implemented, and evaluated. Customers are able to participate, where applicable, in granting access for these roles. The process is designed to ensure that only authorized individuals are granted access to these roles. The process is also designed to help ensure that the risk associated with granting access to these roles is minimized. The process is evaluated regularly to ensure that it continues to meet the organization's security needs.

Question ID	Question	CSP CAIQ Answer
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	NA

IAM-12 - Safeguard Logs Integrity

Control Specifications

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.

Implementation Description

Exoscale logging infrastructure access is restricted to a limited set of team members. Logs are stored in 2 different systems including an offsite encrypted copy with non-overlapping team members access ensuring that a log entry cannot be simply deleted by a single person. The ability to disable the "read-only" configuration of log archive infrastructure is controlled through a procedure that ensures the segregation of duties and break glass procedures. The segregation of duties procedure ensures that only authorized personnel have the ability to make changes to the logging infrastructure, while the break glass procedure allows authorized personnel to make changes to the logging infrastructure in the event of an emergency.

Question ID	Question	CSP CAIQ Answer
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	No
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	No

IAM-13 - Uniquely Identifiable Users

Control Specifications

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.

Implementation Description

Unique identifiers (UIDs) and personal key digests are used to ensure that users are identifiable and that their usage can be associated with them. The UID is a randomly generated number that is unique to each user. The personal key digest is a cryptographic hash of the user's personal key, which is also unique to each user. These identifiers are used to track user activity and to ensure that the system is functioning properly.

Question ID	Question	CSP CAIQ Answer
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes

IAM-14 - Strong Authentication

Control Specifications

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.

Implementation Description

Exoscale employs a variety of methods for authenticating access to systems, applications, and data assets. These methods include username and password authentication, two-factor authentication (2FA), client certificate and key-based authentication, and others. These methods are all implemented and evaluated to ensure that the least amount of privilege is granted to users and that sensitive data is accessed only by authorized individuals. Digital certificates are used for machine to machine communication. Alternatives that achieve an equivalent security level are not typically adopted, as digital certificates provide a higher level of security.

Question ID	Question	CSP CAIQ Answer
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes

IAM-15 - Passwords Management

Control Specifications

Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.

Implementation Description

Processes, procedures, and technical measures for the secure management of passwords are defined, implemented, and evaluated. For example, employees are mandated to use a password manager, and company wide secrets are securly stored in an encrypted form.

Question ID	Question	CSP CAIQ Answer
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes

IAM-16 - Authorization Mechanisms

Control Specifications

Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.

Implementation Description

Access to data and system functions are authorized, defined, implemented, and evaluated on a role-based / need to know basis. Role-based access control (RBAC) is a method of restricting system access to authorized users, processes, or objects. RBAC is based on the principle of least privilege, which means that users are granted only the minimum privileges they need to perform their jobs. In RBAC, each user is assigned a role, and the role defines the user

Question ID	Question	CSP CAIQ Answer
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes

INTEROPERABILITY & PORTABILITY

IPY-01 - Interoperability and Portability Policy and Procedures

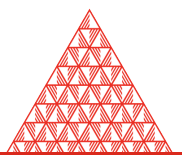
Control Specifications

Establish, document, approve, communicate, apply, evaluate and maintainpolicies and procedures for interoperability and portability includingrequirements for:a. Communications between application interfacesb. Information processing interoperabilityc. Application development portabilityd. Information/Data exchange, usage, portability, integrity, and persistenceReview and update the policies and procedures at least annually.

Implementation Description

Exocale provides extensive documentation for it's API on community.exoscale.com. This documentation covers how to use the API, what endpoints are available, and what parameters are accepted. Exocale also has a Developer Portal where developers can register for an account and get access to a range of resources, including API keys. Exoscale's policies and procedures for information processing interoperability are not currently established, documented, approved, communicated, applied, evaluated, or maintained. However, our terms and conditions do specify that we will return data in a standard industry format upon customer request. We currently support the import and export of data in QCOW2 format for virtual machine images. Development teams are encouraged to use open source and reusable components, frameworks, and libraries to promote code portability. Automated code scanning and analysis tools are used to identify potential portability issues and to recommend corrective actions. Development teams are also encouraged to use standard coding practices and to develop modular code that can be easily ported to different platforms. Exoscale does not have a formal policy governing information and data exchange and portability but ensure its customer are not locked-in the plaform by supporting common standard API and data format. Exoscale does not have a formal policy governing information and data exchange and portability but ensure its customer are not locked-in the plaform by supporting common standard API and data format.

Question ID	Question	CSP CAIQ Answer
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	No



Question ID	Question	CSP CAIQ Answer
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	No
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	No
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	No

IPY-02 - Application Interface Availability

Control Specifications

Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.

Implementation Description

Exoscale offer an application programming interface (API) that enables interoperability and portability. This means that data can be programmatically accessed and retrieved, enabling CSCs to work with other applications and systems.

Question ID	Question	CSP CAIQ Answer
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes

IPY-03 - Secure Interoperability and Portability Management

Control Specifications

Implement cryptographically secure and standardized network protocols for the management, import and export of data.

Implementation Description

All data transfer between systems occurs over cryptographically secure network protocols. This ensures that data is transmitted securely and that it cannot be compromised en route. Additionally, all data is standardized so that it can be easily imported and exported between systems. This ensures that data can be easily shared between teams and systems.

Question ID	Question	CSP CAIQ Answer
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes

IPY-04 - Data Portability Contractual Obligations

Control Specifications

Agreements must include provisions specifying CSCs access to dataupon contract termination and will include:a. Data formatb. Length of time the data will be storedc. Scope of the data retained and made available to the CSCsd. Data deletion policy

Implementation Description

Data access upon contract termination is specified in Clause 13.5 of Exoscale T&Cs. The data format, duration data will be stored, and scope of data retained and made available to CSCs are also specified in the agreement. The data deletion policy is also outlined in the agreement.

Question ID	Question	CSP CAIQ Answer
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following?a. Data formatb. Duration data will be storedc. Scope of the data retained and made available to the CSCsd. Data deletion policy	Yes

INFRASTRUCTURE & VIRTUALIZATION SECURITY

IVS-01 - Infrastructure and Virtualization Security Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has a comprehensive set of policies and procedures as part of its operational operations documentation. These policies and procedures are applied to the company's infrastructure and virtualization security. They are also communicated to employees and customers, and are regularly evaluated and updated. Exoscale policies and procedures are reviewed yearly. This helps ensure that our infrastructure and virtualization security policies and procedures are up-to-date and effective.

Question ID	Question	CSP CAIQ Answer
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes

IVS-02 - Capacity and Resource Planning

Control Specifications

Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.

Implementation Description

Exoscale conducts capacity monitoring and planning on an ongoing basis as described in its Capacity Planning documentation. This includes regular reviews of resource availability, quality, and capacity to ensure that the system performance required by the business is delivered.

Question ID	Question	CSP CAIQ Answer
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes

IVS-03 - Network Security

Control Specifications

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.

Implementation Description

Authorized flow between machines are monitored for authorized traffic flow attempts. Any unauthorized traffic is blocked and reported. Communication between environments are encrypted and authenticated. Communication between environments are restricted by default and only permitted as justified by the business. This ensures that only authenticated and authorized connections are allowed, which helps protect sensitive data and systems. Network configuration changes undergo a review and validation process before being activated. However, there is no mandatory yearly review of network configurations. Active network configurations are regularly reviewed, but the frequency varies depending on the changes made and the criticality of the systems. All network configurations have a documented history of matching business requirements. This is done through a combination of automated and manual processes, as well as regular audits of the network. Any changes to the network are logged and tracked, and only changes that are approved through the change management process are allowed. This helps ensure that all network activity is justified and meets the organization's security and compliance requirements.

Question ID	Question	CSP CAIQ Answer
IVS-03.1	Are communications between environments monitored?	Yes
IVS-03.2	Are communications between environments encrypted?	Yes
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes
IVS-03.4	Are network configurations reviewed at least annually?	No
IVS-03.5	Are network configurations supported by the documented justification of	Yes

Question ID	Question	CSP CAIQ Answer
	all allowed services, protocols, ports, and compensating controls?	

IVS-04 - OS Hardening and Base Controls

Control Specifications

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.

Implementation Description

All hosts use hardened base OS configurations. Technical controls are in place to support security baselines for hosts and guests. These technical controls are part of an overall security management program that is designed to protect the infrastructure and data.

Question ID	Question	CSP CAIQ Answer
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes

IVS-05 - Production and Non-Production Environments

Control Specifications

Separate production and non-production environments.

Implementation Description

Production and non-production are separated logically. In most cases, production is physically segregated from non-production. This helps ensure that production systems are not impacted by changes made to non-production systems.

Question ID	Question	CSP CAIQ Answer
IVS-05.1	Are production and non-production environments separated?	Yes

IVS-06 - Segmentation and Segregation

Control Specifications

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.

Implementation Description

Technical measures are in place to guaranty the proper segmentation of intra-tenant infrastructure. This includes proper firewalling and routing, as well as segregated storage and compute resources. Access is also restricted based on role, so that users within a tenant have only the access they need to perform their tasks. Monitoring and logging is also in place to detect and report any violations of segmentation.

Question ID	Question	CSP CAIQ Answer
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes

IVS-07 - Migration to Cloud Environments

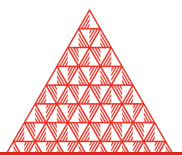
Control Specifications

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.

Implementation Description

Cryptography is used to protect information in transit between devices and to protect data at rest. All communication channels between devices are cryptographically secured using approved protocols. Data is encrypted using approved algorithms and keys are protected using approved key management techniques.

Question ID	Question	CSP CAIQ Answer
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes



IVS-08 - Network Architecture Documentation

Control Specifications

Identify and document high-risk environments.

Implementation Description

Exoscale is currently not formally identified as a high-risk environment and no specific components are noted as high-risk. However, the integrality of the Exoscale platform is currently recognized as a high-risk environment with no distinction within it's components. Additional assessment and documentation of specific high-risk components and environments is recommended.

Question ID	Question	CSP CAIQ Answer
IVS-08.1	Are high-risk environments identified and documented?	No

IVS-09 - Network Defense

Control Specifications

Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.

Implementation Description

Processes, procedures, and defense-in-depth techniques are defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks. The organization has detection and mitigation capabilities in place to protect against DDoS attacks.

Question ID	Question	CSP CAIQ Answer
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

LOGGING AND MONITORING

LOG-01 - Logging and Monitoring Policy and Procedures

Control Specifications

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.

Implementation Description

Our logging and monitoring policies and procedures are established, documented, approved, communicated, applied, evaluated, and maintained. We have a formal process for creating and maintaining our internal operations documentation, which includes our logging and monitoring policies and procedures. This process is managed by our operations team, and all changes to the documentation are tracked and approved by senior management. Exoscale policies and procedures are reviewed yearly.

Question ID	Question	CSP CAIQ Answer
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes

LOG-02 - Audit Logs Protection

Control Specifications

Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.

Implementation Description

Processes, procedures, and technical measures are in place to ensure audit log security and retention. The logs are centralized and immediately stored in 2 different systems, which prevents any tampering or loss of data. Security measures are also in place to restrict access to the logs only to authorized personnel.

Question ID	Question	CSP CAIQ Answer
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes

LOG-03 - Security Monitoring and Alerting

Control Specifications

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.

Implementation Description

Exoscale employs a comprehensive monitoring and alerting infrastructure allowing for the identification of security-related events. This infrastructure includes a variety of sensors (e.g. firewalls, intrusion detection/prevention systems, performance and availability monitoring, etc.) that feed data into a centralized monitoring system. This system analyzes the data to identify potential security incidents, and generates alerts (via email, SMS, or other mechanisms) to notify appropriate personnel. A system can be defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics. Alerts rules can be defined based on security-related events or metrics. For example, a rule could be defined to generate an alert when the average response time for a particular application exceeds a certain threshold.

Question ID	Question	CSP CAIQ Answer
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes

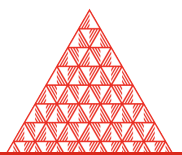
LOG-04 - Audit Logs Access and Accountability

Control Specifications

Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.

Implementation Description

Access to the audit logs is restricted to authorized personnel. The audit logs are used to



track access to the system and to provide accountability for changes made to the system. Records are maintained to track which users have accessed the audit logs and to ensure that only authorized personnel have access to the information.

Question ID	Question	CSP CAIQ Answer
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes

LOG-05 - Audit Logs Monitoring and Response

Control Specifications

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.

Implementation Description

Security logs are regularily reviewed for unusual activity patterns. This is done in order to detect any activity that falls outside of the typical or expected patterns. This helps to ensure the security of the organization's systems and data. Exoscale has an established Incident Management procedures to follow upon anomaly detection. The 5 stages process is: Plan and prepare, Detection and reporting, Assessment and decision, Treatment, Learn / Document. This process is followed to review and take appropriate and timely actions on detected anomalies.

Question ID	Question	CSP CAIQ Answer
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes

LOG-06 - Clock Synchronization

Control Specifications

Use a reliable time source across all relevant information processing systems.

Implementation Description

Exoscale uses the Network Time Protocol (NTP) to synchronize its time source. This ensures that all relevant information processing systems have a reliable time source.

Question ID	Question	CSP CAIQ Answer
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes

LOG-07 - Logging Scope

Control Specifications

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.

Implementation Description

Logging requirements are defined on an application by application basis, and specific to the needs of the system. Events that are logged typically include information such as user ID, timestamp, and the action that was taken. The scope of the policy is reviewed and updated at least bi-annually, or whenever there is a change in the threat environment.

Question ID	Question	CSP CAIQ Answer
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	No

LOG-08 - Log Records

Control Specifications

Generate audit records containing relevant security information.

Implementation Description

Exoscale does not generate audit records. All log records are stored in a log collection and analysis tool. Logs are enriched with metadata that can be leveraged for security event analysis.

Question ID	Question	CSP CAIQ Answer
LOG-08.1	Are audit records generated, and do they contain relevant security information?	No

LOG-09 - Log Protection

Control Specifications

The information system protects audit records from unauthorized access, modification, and deletion.

Implementation Description

The information system protects audit records from unauthorized access, modification, and deletion. Access to the logging infrastructure is restricted to authorized personnel. Operational logs are ingested and stored securely, and are archived off site encrypted and with access restricted to a subset of the personnel.

Question ID	Question	CSP CAIQ Answer
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes

LOG-10 - Encryption Monitoring and Reporting

Control Specifications

Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.

Implementation Description

Exoscale maintain a comprehensive documentation if its PKI infrastructure and has a published cryptography policy in place. This policy covers all aspects of cryptography operations, from the generation of encryption keys, to their use and storage. Exoscale also has in place a comprehensive system for internal reporting on all aspects of its cryptographic operations. This system includes both automated reporting and manual review of key management processes and controls.

Question ID	Question	CSP CAIQ Answer
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes

LOG-11 - Transaction/Activity Logging

Control Specifications

Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.

Implementation Description

All key lifecycle events are logged and monitored in order to enable auditing and reporting on cryptographic keys' usage. Our internal cryptography policy requires that all key lifecycle events be logged and monitored in order to ensure that cryptographic keys are being used in a manner that is consistent with our security and risk management requirements.

Question ID	Question	CSP CAIQ Answer
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	No

LOG-12 - Access Control Logs

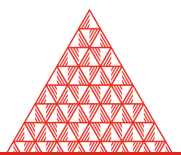
Control Specifications

Monitor and log physical access using an auditable access control system.

Implementation Description

All access to Exoscale datacenters is logged and auditable. Access to our facilities is restricted to authorized personnel only. All access is logged and tracked, including who accessed the facility, when they accessed it, and from where.

Question ID	Question	CSP CAIQ Answer
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes



LOG-13 - Failures and Anomalies Reporting

Control Specifications

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.

Implementation Description

Exoscale have a process and technical measures to report monitoring system anamolies. This includes event processing and alerting. Exoscale's event processing system monitors all activity on the platform and records events in a central repository. This repository is used to generate alerts, which are sent to the appropriate personnel. Exoscale notify all affected parties of any data incidents that affect them. This is described in more detail in the Exoscale data privacy handbook.

Question ID	Question	CSP CAIQ Answer
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes

SECURITY INCIDENT MANAGEMENT, E-DISCOVERY, & CLOUD FORENSICS

SEF-01 - Security Incident Management Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has an incident management procedures as part of it's ISMS. This includes procedures for managing security incidents, e-discovery, and cloud forensics. The procedures are established, documented, approved, communicated, applied, evaluated, and maintained. Incident management policies are reviewed annually as part of the ISMS review. The review is conducted to ensure that the policies are effective and continue to meet the organization's needs. Any updates or changes to the policies are made as necessary.

Question ID	Question	CSP CAIQ Answer
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes

SEF-02 - Service Management Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has developed a policy and procedures for the timely management of security incidents. The policy and procedures specify service level objectives that ensure that

incidents are dealt with in a timely fashion, depending on the incident severity. The policy and procedures are documented, approved, communicated, applied, evaluated, and maintained. Incident management policies are reviewed annually as part of the ISMS review. The review process includes an assessment of the adequacy of the policies and procedures and their effectiveness in achieving the organization's security objectives. Any necessary updates are made to ensure that the policies and procedures continue to meet the organization's needs.

Question ID	Question	CSP CAIQ Answer
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes

SEF-03 - Incident Response Plans

Control Specifications

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.

Implementation Description

Exoscle has a Outage & emergency response procedure plan that is followed in the event of an incident. This plan includes the relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain). The plan is documented, approved, communicated, applied, evaluated, and maintained.

Question ID	Question	CSP CAIQ Answer
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes

SEF-04 - Incident Response Testing

Control Specifications

Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.

Implementation Description

Exoscale conducts business continuity drills on a regular basis to assess the effectivness of it's incident response plan as well as its business continuity procerdures. In the event of a significant organizational or environmental change, the security incident response plan would be updated as necessary.

Question ID	Question	CSP CAIQ Answer
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes

SEF-05 - Incident Response Metrics

Control Specifications

Establish and monitor information security incident metrics.

Implementation Description

All incidents are recorded and monitored using security related KPI. This allows us to track the frequency and severity of incidents, and take corrective action where necessary.

Question ID	Question	CSP CAIQ Answer
SEF-05.1	Are information security incident metrics established and monitored?	Yes

SEF-06 - Event Triage Processes

Control Specifications

Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.

Implementation Description

There are defined processes for triaging and evaluating security related events. These processes are implemented and evaluated regularly to ensure that they are effective in identifying and addressing security issues. Technical measures are in place to support these processes and help ensure that security-related events are properly triaged and addressed.

Question ID	Question	CSP CAIQ Answer
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes

SEF-07 - Security Breach Notification

Control Specifications

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.

Implementation Description

Technical measures are in place to notify CSC of security or data breach incidents. Security breaches are reported externally as per applicable laws and regulations as documented in our internal privacy handbook. Security breaches and assumed security breaches are tracked and reported to our senior leadership team and the board of directors.

Question ID	Question	CSP CAIQ Answer
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes

SEF-08 - Points of Contact Maintenance

Control Specifications

Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.

Implementation Description

Points of contact are maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. Contact details are documented in our internal documentation.

Question ID	Question	CSP CAIQ Answer
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes

SUPPLY CHAIN MANAGEMENT, TRANSPARENCY, AND ACCOUNTABILITY

STA-01 - SSRM Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has policies and procedures in place that implement the SSRM. Our roles and responsibilities are documented on our Security page at https://www.exoscale.com/security/, and our terms and conditions communicate our security expectations to tenants. Our policies and procedures are applied and evaluated regularly, and we maintain a continuous improvement process to ensure that our security posture meets the latest industry standards. Exoscale reviews and updates the SSRM policies and procedures annually. Exoscale documents SSRM ownership for each security control and reviews this documentation yearly.

Question ID	Question	CSP CAIQ Answer
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes

STA-02 - SSRM Supply Chain

Control Specifications

Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.

Implementation Description

Exoscale's Terms and Conditions (T&Cs) and documentation make clear the shared

responsibility of the cloud provider and the cloud customer in the context of iaas and paas. The SSRM is applied, documented, implemented, and managed throughout the supply chain for the cloud service offering.

Question ID	Question	CSP CAIQ Answer
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes

STA-03 - SSRM Guidance

Control Specifications

Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.

Implementation Description

Exoscale's Terms and Conditions and documentation make clear the shared responsibility of the cloud provider and the cloud customer in the context of iaas and paas.

Question ID	Question	CSP CAIQ Answer
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes

STA-04 - SSRM Control Ownership

Control Specifications

Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.

Implementation Description

The shared ownership and applicability of all CSA CCM controls are delineated according to the SSRM for the cloud service offering.

Question ID	Question	CSP CAIQ Answer
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

STA-05 - SSRM Documentation Review

Control Specifications

Review and validate SSRM documentation for all cloud services offerings the organization uses.

Implementation Description

Exoscale's Terms and Conditions (T&Cs) and public documentation are peer-reviewed and validated before being published. Updates to our T&Cs and public documentation are also peer-reviewed and validated.

Question ID	Question	CSP CAIQ Answer
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes

STA-06 - SSRM Control Implementation

Control Specifications

Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.

Implementation Description

The portions of the SSRM that the organization is responsible for are implemented, operated, audited, and assessed. Exoscale undergoes accredited certification audits yearly for information security management.

Question ID	Question	CSP CAIQ Answer
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes

STA-07 - Supply Chain Inventory

Control Specifications

Develop and maintain an inventory of all supply chain relationships.

Implementation Description

Exoscale maintains an inventory of all third-party providers in its supply chain. This inventory includes information on the providers' capabilities and services. Exoscale regularly reviews this inventory to ensure that it has the most up-to-date information on

its supply chain partners.

Question ID	Question	CSP CAIQ Answer
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes

STA-08 - Supply Chain Risk Management

Control Specifications

CSPs periodically review risk factors associated with all organizations within their supply chain.

Implementation Description

CSPs periodically review the risk factors associated with all organizations within the supply chain. This includes third-party suppliers and their associated risks. This is done on a yearly basis in order to ensure that the CSP is aware of any changes that may have occurred and to make sure that the CSP is still comfortable with the risk levels associated with these organizations.

Question ID	Question	CSP CAIQ Answer
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes

STA-09 - Primary Service and Contractual Agreement

Control Specifications

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

Implementation Description

Our service agreements with 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

Question ID	Question	CSP CAIQ Answer
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms?• Scope, characteristics, and location of business relationship and services offered• Information security requirements (including SSRM)• Change management process• Logging and monitoring capability• Incident management and communication procedures• Right to audit and third-party assessment• Service termination• Interoperability and portability requirements• Data privacy	Yes

STA-10 - Supply Chain Agreement Review

Control Specifications

Review supply chain agreements between CSPs and CSCs at least annually.

Implementation Description

Exoscale does not have a supply chain agreement with tenants.

Question ID	Question	CSP CAIQ Answer
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	NA

STA-11 - Internal Compliance Testing

Control Specifications

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.

Implementation Description

Exoscale's Compliance Team conducts an annual assessment of the conformance and effectiveness of standards, policies, procedures, and SLA activities. This assessment helps to ensure that Exoscale is meeting its obligations and providing the highest quality of service to its customers.

Question ID	Question	CSP CAIQ Answer
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes

STA-12 - Supply Chain Service Agreement Compliance

Control Specifications

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.

Implementation Description

Our 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 are implemented. Third party vendor security is reviewed and evaluated annually for compliance against our information security and privacy policies.

Question ID	Question	CSP CAIQ Answer
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes

STA-13 - Supply Chain Governance Review

Control Specifications

Periodically review the organization's supply chain partners' IT governance policies and procedures.

Implementation Description

Exoscale maintains a third party security policy that is reviewed annually. In addition, they conduct annual reviews of their supplier policies. This helps ensure that their supply chain partners are adhering to the same high security standards that Exoscale holds itself to.

Question ID	Question	CSP CAIQ Answer
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes

STA-14 - Supply Chain Data Security Assessment

Control Specifications

Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.

Implementation Description

Exoscale third party security policy mandates that third party providers security must be assessed once a year.

Question ID	Question	CSP CAIQ Answer
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes

THREAT & VULNERABILITY MANAGEMENT

TVM-01 - Threat and Vulnerability Management Policy and Procedures

Control Specifications

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.

Implementation Description

Exoscale has a formal vulnerability management process in place that includes the identification, assessment, and remediation of vulnerabilities. Vulnerabilities are prioritized and remediated in accordance with the risk they pose to the environment. Patch management processes are in place to ensure that systems are kept up to date with the latest security patches.

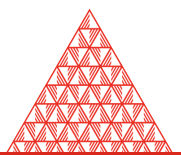
The vulnerability management process is regularly reviewed and updated as needed to ensure that it is effective in identifying and mitigating vulnerabilities. Exoscale's Vulnerability Management Policy and Incident Management Procedure is reviewed yearly as part of the ISMS review.

Question ID	Question	CSP CAIQ Answer
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes

TVM-02 - Malware Protection Policy and Procedures

Control Specifications

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.



Implementation Description

Exoscale has policies and procedures to protect against malware. Malware detection are mandated on system subjected to receive content from external sources (mail system, file-sharing...). Exoscale security policies are reviewed during the bi-annual ISMS review.

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

TVM-03 - Vulnerability Remediation Schedule

Control Specifications

Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.

Implementation Description

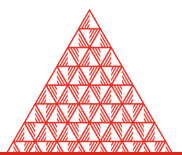
Scheduled and emergency procedures are defined and implemented according to our Vulnerability Management Policy and Incident Management Procedures. Technical measures are also defined and implemented according to our Security Policy and related standards. Processes and procedures are evaluated on a regular basis to ensure that they are effective in enabling us to respond to identified vulnerabilities.

Question ID	Question	CSP CAIQ Answer
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes

TVM-04 - Detection Updates

Control Specifications

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.



Implementation Description

Exoscale has a published Vulnerability Management Policy and monitors continuously its exposure to external threats.

Question ID	Question	CSP CAIQ Answer
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes

TVM-05 - External Library Vulnerabilities

Control Specifications

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.

Implementation Description

Exoscale monitors its supply chain vulnerability exposures using automated tools to identify updates and new vulnerabilities that could affect its systems. Updates to Exoscale's systems are managed through a change management process that includes a formal evaluation of the potential impacts of proposed changes.

Question ID	Question	CSP CAIQ Answer
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes

TVM-06 - Penetration Testing

Control Specifications

Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.

Implementation Description

Exoscale uses 3rd party pentesters to conduct penetration tests on an annual-basis. In addition, Exoscale has a permenant bug bounty program to reward responsible disclosure from the security community.

Question ID	Question	CSP CAIQ Answer
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes

TVM-07 - Vulnerability Identification

Control Specifications

Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.

Implementation Description

Exoscale has a published Vulnerability Management Policy and monitors continuously its exposure to external threats. Procedures and technical measures are defined, implemented and evaluated for vulnerability detection on organizationally managed assets at least monthly.

Question ID	Question	CSP CAIQ Answer
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes

TVM-08 - Vulnerability Prioritization

Control Specifications

Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.

Implementation Description

Exoscale employs a risk management methodology based on the WISE framework. The WISE framework is an industry-recognized framework that provides a comprehensive and systematic approach to risk assessment and management. The framework includes a risk assessment methodology, a risk management process, and a risk-based decision-making framework.

Question ID	Question	CSP CAIQ Answer
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from	Yes

Question ID	Question	CSP CAIQ Answer
	an industry-recognized framework?	

TVM-09 - Vulnerability Management Reporting

Control Specifications

Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.

Implementation Description

Exoscale logs and tracks all vulnerabilities and remediations activities. Affected tenants are notified as documented in our data privacy handbook.

Question ID	Question	CSP CAIQ Answer
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes

TVM-10 - Vulnerability Management Metrics

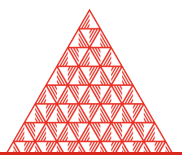
Control Specifications

Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.

Implementation Description

Exoscale uses key performance indicators (KPIs) to measure the effectiveness of its information security management system (ISMS). These KPIs include metrics regarding the identification and remediation of vulnerabilities. Exoscale monitors these KPIs at defined intervals to ensure that its ISMS is effective in mitigating vulnerabilities.

Question ID	Question	CSP CAIQ Answer
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes



UNIVERSAL ENDPOINT MANAGEMENT

UEM-01 - Endpoint Devices Policy and Procedures

Control Specifications

Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.

Implementation Description

Procedure and policies regarding the access of any part of Exoscale production infrastructure are documented. Accesss to production system using mobile or personnal devices is forbidden. Exoscale ISMS policies are reviewed during the bi-annual ISMS review.

Question ID	Question	CSP CAIQ Answer
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes

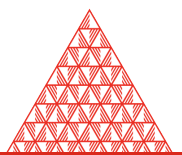
UEM-02 - Application and Service Approval

Control Specifications

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.

Implementation Description

The organization has a defined, documented, and applicable list of approved cloud services that are acceptable for use by endpoints when accessing or storing organization-managed data. This list is maintained as part of the Employee Confidentiality policies. RBAC is used to restrict access to these services on a need to have basis.



Question ID	Question	CSP CAIQ Answer
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes

UEM-03 - Compatibility

Control Specifications

Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.

Implementation Description

A process is defined and implemented to validate endpoint device compatibility with operating systems and applications. Mobile devices accessing corporate data are mandated to support the Google MDM solution. This process ensures that all devices accessing corporate data are managed and compliant with corporate security policies.

Question ID	Question	CSP CAIQ Answer
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes

UEM-04 - Endpoint Inventory

Control Specifications

Maintain an inventory of all endpoints used to store and access company data.

Implementation Description

All companies issued endpoints are recorded and tracked in our inventory management system. This helps us to ensure that only authorized devices are used to access company data, and that all devices are up-to-date with the latest security patches. We also use this information to generate reports on endpoint usage, so that we can identify any devices that are not being used or that are no longer needed.

Question ID	Question	CSP CAIQ Answer
UEM-04.1	Is an inventory of all endpoints used and maintained to store and	Yes

Question ID	Question	CSP CAIQ Answer
	access company data?	

UEM-05 - Endpoint Management

Control Specifications

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.

Implementation Description

Exoscale's information classification policy document defines the appropriate handling rules for organization data. This includes storage and transmission procedures which are enforced through processes, procedures, and technical measures. These controls are implemented and evaluated for all endpoints permitted to access systems and/or store, transmit, or process organizational data.

Question ID	Question	CSP CAIQ Answer
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes

UEM-06 - Automatic Lock Screen

Control Specifications

Configure all relevant interactive-use endpoints to require an automatic lock screen.

Implementation Description

All relevant interactive-use endpoints are configured to require an automatic lock screen. This is mandated by our internal Employee Confidentiality Policies.

Question ID	Question	CSP CAIQ Answer
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes

UEM-07 - Operating Systems

Control Specifications

Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.

Implementation Description

Changes to endpoint operating systems, patch levels, and/or applications are managed through the organizational change management process. Exoscale policy mandates that all endpoints must be updated in the event of the release of updates that include security fixes.

Question ID	Question	CSP CAIQ Answer
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes

UEM-08 - Storage Encryption

Control Specifications

Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.

Implementation Description

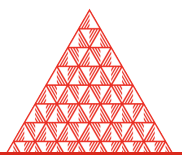
Exoscale policy mandates the use of full disk encryption on all employee controlled endpoints including laptops and mobile devices. This ensures that any sensitive data stored on the device is protected from unauthorized access or disclosure, even if the device is lost or stolen.

Question ID	Question	CSP CAIQ Answer
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes

UEM-09 - Anti-Malware Detection and Prevention

Control Specifications

Configure managed endpoints with anti-malware detection and prevention technology and services.



Implementation Description

All employees using Microsoft Windows as their Operating System are mandated to have anti-malware detection technology installed and configured on their device. Endpoints that are company issued Windows laptops are fully managed and protected against malware.

Question ID	Question	CSP CAIQ Answer
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes

UEM-10 - Software Firewall

Control Specifications

Configure managed endpoints with properly configured software firewalls.

Implementation Description

Software firewalls are configured on managed endpoints. Company issued endpoints are required to have software firewalls enabled and properly configured in order to comply with our security policies.

Question ID	Question	CSP CAIQ Answer
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes

UEM-11 - Data Loss Prevention

Control Specifications

Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.

Implementation Description

Exoscale's file-sharing system offers DLP features with rules triggering alerts in the event of suspicious behaviour from a user. These rules are reviewed regularly to ensure that the system is effective in protecting data.

Question ID	Question	CSP CAIQ Answer
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes

UEM-12 - Remote Locate

Control Specifications

Enable remote geo-location capabilities for all managed mobile endpoints.

Implementation Description

Mobile devices are not allowed to access the Exoscale production infrastructure.

Question ID	Question	CSP CAIQ Answer
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes

UEM-13 - Remote Wipe

Control Specifications

Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.

Implementation Description

The mobile devices accessing corporate data are mandated to support the Google MDM solution which supports remote data deletion. The processes, procedures, and technical measures are defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices.

Question ID	Question	CSP CAIQ Answer
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes

UEM-14 - Third-Party Endpoint Security Posture

Control Specifications

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.