CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB maintains appropriate documented information as evidence of monitoring and measurement results, according to 27001:9.2.				A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.							
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	SEEWEB's approach to information security management and its implementation are independently reviewed at planned intervals or when significant changes occur, according to 27001: A.18.2.1.				A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	SEEWEB internal and external audit and assurance uses risk-based plans and approach to conduct assessments at least annually.				A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	SEEWEB maintains compliance with internal and external parties to verity, monitor legal, regulatory, and contractual requirements, according to 27001: A.18.2.2, A.18.2.3.				A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	Audits are planned and performed to review the continuous improvement of SEEWEB against standards-based criteria, according to 27001: A.18.2.2.				A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	In alignment with ISO 27001, SEEWEB maintains a Risk Management program to mitigate and manage risk.				A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	SEEWEB has established a formal audit program that includes continual, independent internal and external assessments.							
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	CSP-owned	SEEWEB has established formal policies and procedures to provide a common baseline for information security standards and guidance, according to 27001: A.14.2.1, 14.2.5.				AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.							
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	SEEWEB maintains a approach, to planning and developing new services, to ensure the quality and security requirements, according to 27001: A.5.1.1, A.7.2.2.				AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	SEEWEB leadership regularly review compliance with policies, standards, and any other appropriate security requirements, according to 27001: A.18.2.2.				AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	SEEWEB complies with information system security and security requirements in development and support processes, according to 27001: A.14.1.1, A.14.1.2, A.14.2.1				AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	SEEWEB implements a testing strategy, including criteria for acceptance and upgrades, according to 27001: A14.1.1, A.14.2.2, A.14.2.8, A.14.2.9				AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	When applicable, a deployment methodology is conducted by SEEWEB to ensure changes are automated, eliminating as many manual steps as possible.							

AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	SEEWEB has established rules for software and systems development and applies them to developments within the organization.	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Where possibile, SEEWEB automates the deployment and integration of application code.	
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	SEEWEB manages technical vulnerabilities and responds to security incidents in accordance with 27001: A.12.6.1, A.16.1.5	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	When possibile, SEEWEB automates remediate of application security vulnerability.	
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB has established, documents, implements, and maintains processes, procedures, and controls to ensure the level of continuity required for information security during an adverse situation in accordance with 27001: A.17.1.2	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and CSC	SEEWEB Business Continuity Policies and Plans have been developed and tested in alignment with 27001: A.17.1.2.	Service interruptions are managed and reported thanks to the monitoring of the sub system services.
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	Shared CSP and CSC	SEEWEB Business Continuity Policies and Plans have been developed and tested in alignment with 27001: A.17.1.	View response to BCR-02.1.
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	Shared CSP and CSC	SEEWEB Business Continuity Policies and Plans have been developed and tested in alignment with 27001: A.17.1.1, A.17.1.3.	View response to BCR-02.1.
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	The SEEWEB business continuity plan details the approach to recover and reconstitute its infrastructure.	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Information system documentation is available internally to SEEWEB personnel through the use of internal documentation system.	
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Test business continuity plan are made by SEEWEB at least annually or as needed basis, in accord to 27001: A.17.1.3.	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	The SEEWEB Business Continuity policy define communication with stakeholders and participants.	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	SEEWEB maintains a retention policy applicable to its internal data and system components, replicated geographically.	In addition to the regular backups by the SeeWeb provider, additional daily backups of the Databases are foreseen
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	SEEWEB maintains a retention policy applicable to its internal data and system components, replicated geographically.	In addition to the regular backups by the SeeWeb provider, additional daily backups of the Databases are foreseen. Integrity checks of the Databases are expected
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSC-owned	-	SEEWEB allows customers to centrally manage and automate backups across its services.Backups can be restored manually

AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	Business Continuity Management and Operational Resilience
BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	
BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	
BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	

BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	Shared CSP and CSC	SEEWEB has established, documents, implements, and maintains processes, procedures, and controls to ensure the level of continuity required during an adverse situation in accordance with 22301.
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Test disaster response plan are made by SEEWEB at least annually or as needed basis, in accord to 22301: 8.5.
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	-
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	CSP-owned	Each data center is built to physical, environmental, and security standards, employing a redundancy model to ensure system availability in the event of component failure.
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	SEEWEB controls changes to the organization, business processes, information processing facilities, and systems that could affect information security, in accorde to 27001: A.12.1.2
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	SEEWEB keeps track of changes to systems within the life cycle through the use of formal change control procedures, in accord to 27001: A.14.2.2.
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	In addition to the points above, SEEWEB has defined and appropriately protects secure development environments for systems development and integration initiatives covering the entire systems development cycle.
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Authorized staff must pass two-factor authentication to access data center. Physical access points to server locations are recorded by closed circuit television camera.
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	CSP-owned	SEEWEB notifies to customers changes to the service offering in accordance with the Customer Agreement.
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	SEEWEB keeps track of changes to systems within the life cycle through the use of formal change control procedures, in accord to 27001: A.14.2.2.
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	No	CSP-owned	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	SEEWEB monitors changes to the organization, business processes, information processing facilities, and systems that could affect information security, in accord to 27001: A.12.1.2. The procedure handles
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	View response to CCC-08.1.
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	View response to CCC-08.1.

BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	
CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	

CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	SEEWEB manages cryptographic keys for required cryptography employed within the its infrastructure (GEOTRUST SSL 256 bit, STRONGSWAN IPSEC 256 bit), in accord to 27001:A.10.1.	Access to the data of individual tenants / customers is encrypted and password protected. Passwords are hashed before storing them in the database. All communications between browsers and
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	Shared CSP and CSC	View response to CEK-01.1.	View response to CEK-01.1.
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSC-owned		View response to CEK-01.1.
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSC-owned		View response to CEK-01.1.
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	Shared CSP and CSC	View response to CEK-01.1.	View response to CEK-01.1.
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	Shared CSP and CSC	View response to CEK-01.1.	View response to CEK-01.1.
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	CSP-owned	SEEWEB management reviews and evaluates the risks identified in its risk management program.	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	Yes	CSC-owned		
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	SEEWEB's approach to information security management and its implementation are independently reviewed at planned intervals or when significant changes occur. Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	View response to CEK-09.1.	
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and CSC	View response to CEK-01.1.	View response to CEK-01.1.
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	CSC-owned		View response to CEK-01.1.
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSC-owned		Cryptographic keys are rotated every 3 months
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	NA	CSC-owned		View response to CEK-01.1.
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?	No	CSC-owned		View response to CEK-01.1.

CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	Cryptography, Encryption & Key Management
CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	
CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	

CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned		View response to CEK-01.1.	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned		View response to CEK-01.1.	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned		View response to CEK-01.1.	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	CSC-owned		View response to CEK-01.1.	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	CSC-owned		View response to CEK-01.1.	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and CSC	SEEWEB cryptographic processes are reviewed by independent third-party auditors for our continued compliance with ISO 27001.	View response to CEK-01.1.	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	NA	CSC-owned		View response to CEK-01.1.	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	All SEEWEB equipment containing storage media is checked to ensure that any critical data or licensed software is securely removed or overwritten before disposal or reuse, in accordance with 27001:A.11.2.7.		DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	CSP-owned	When a storage device has reached the end of its useful life, SEEWEB procedures include a decommissioning process.					
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.					
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	CSP-owned	SEEWEB shall ensure that equipment, information or software is not taken off-site without prior authorization in accordance with 27001:A.11.2.5.		DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	CSP-owned	According to SEEWEB procedures, the written authorization of the technical director is required for this purpose.					

DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				Datacenter Security
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	SEEWEB has designed and applies physical security to offices, premises and facilities in accordance with 27001: A.11.3, A.11.5.	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	CSP-owned	SEEWEB shall ensure that media containing information are protected from unauthorized access, misuse, or tampering during transport in accordance with 27001: A.8.3.3.	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	CSP-owned	SEEWEB classifies information in relation to its value, mandatory requirements, and criticality in the event of unauthorized disclosure, in accordance with 27001: A.8.2.1.	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	SEEWEB identifies information processing assets and facilities. An inventory of these assets is compiled and kept up-to-date, in accordance with 27001: A.8.1.1.	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	SEEWEB has defined and uses security perimeters to protect areas containing critical information and information processing facilities, in accordance with 27001: A.11.1.1.	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	View response to DCS-07.1.				
DCS-08.1	Is equipment identification used as a method for connection authentication?	No	CSP-owned		DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	SEEWEB's security areas are protected by appropriate entry controls designed to ensure that only authorized personnel are allowed access, in accordance with 27001: A.11.1.2. Access control records retained,	DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	View response to DCS-09.1.				
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	CSP-owned	SEEWEB provides perimeter surveillance external and internal by means of cameras with recording and retention in accordance with the law.	DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	CSP-owned	SEEWEB's IDS monitors the accesses with local optical/acoustic signaling and remote by radio alarm to security institution.	DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	Power and telecommunication cables used to transport data or support SEEWEB information services are protected from eavesdropping, interference, or damage in accordance with 27001: A.11.2.3.	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	SEEWEB's air conditioning system provides air filtration, internal internal ventilation and cooling thus ensuring the right temperature and sufficient air exchange. The air conditioning system is	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	

DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	SEEWEB equipment is properly maintained to ensure its continued availability and integrity, in accordance with A.11.2.4.	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	CSP-owned	SEEWEB's equipment is arranged and protected for the purpose of reducing risks from environmental threats and hazards, in accordance with 27001: A.11.2.1.	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	SEEWEB has implemented data handling and classification requirements which provide specifications around data encryption, content in transit and during storage, access, retention, physical controls, mobile devices and handling requirements, in accordance with 27001.	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned	View response to DSP-01.2.	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	NA	CSC-owned		Given the nature of the service, no sensitive personal data is collected Users can receive to be permanently deleted, moreover the Admin user of the Tenant can autonomously delete the individual accounts of his competence
DSP-04.1	Is data classified according to type and sensitivity levels?	NA	CSC-owned		View response to DSP-03.1.
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	NA	CSC-owned		View response to DSP-03.1.
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	NA	CSC-owned		View response to DSP-03.1.
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	NA	CSC-owned		View response to DSP-03.1.
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	NA	CSC-owned		View response to DSP-03.1.
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	SEEWEB maintains a systematic approach, to planning and developing new services, to ensure the quality and security requirements are met	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	NA	CSC-owned		View response to DSP-03.1.
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	NA	CSC-owned		View response to DSP-03.1.
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	NA	CSC-owned		View response to DSP-03.1.
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	NA	CSC-owned		View response to DSP-03.1.

DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	Data Security and Privacy Lifecycle Management
DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	
DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	

DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	NA	CSC-owned		View response to DSP-03.1.
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	Shared CSP and CSC	View response to AIS-02.1.	View response to DSP-03.1.
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	NA	CSC-owned		View response to DSP-03.1.
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	NA	CSC-owned		View response to DSP-03.1.
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	CSC-owned		View response to DSP-03.1.
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and CSC	SEEWEB maintains a retention policy applicable to its internal data and system components in order to continue operations of SEEWEB business and services.	View response to DSP-03.1.
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	NA	CSC-owned		View response to DSP-03.1.
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	CSP-owned	SEEWEB's policy prohibits the disclosure of customer content unless we're required to do so to comply with the law, as required by the GDPR.	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	Shared CSP and CSC	View response to DSP-18.1.	View response to DSP-03.1.
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	NA	CSC-owned		View response to DSP-03.1.
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB has established formal policies and procedures to provide employees a common baseline for information security standards and Guidance, in accordance with 27001: 5.1, 5.2, 5.3.	
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	SEEWEB maintains documented information on the risk assessment process related to information security in accordance with 27001: A.6.1.2.	

DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion
DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing
DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing
DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors
DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use
DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion
DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection
DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification
DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location
GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures
GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program

GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	Governance, Risk and Compliance
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	CSP-owned	SEEWEB management has defined and approved information security policies, which are available as documented information, published, and communicated to staff and relevant third parties in accordance with	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	SEEWEB has established an information security management program with designated roles and responsibilities, in accordance with 27001:	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	SEEWEB has defined and assigned all responsibilities related to information security in accordance with 27001: A.6.1.1.	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	SEEWEB complies with mandatory and contractual requirements.	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	SEEWEB maintains appropriate contacts with specialist groups and professional associations attended by information security specialists,	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB conducts background checks on all employment candidates in accordance with relevant laws, regulations, and ethics; these are proportionate to business needs, classification of information to be accessed, and perceived risks, in accordance with 27001:A.7.1.1.	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	View response to HRS-01.1.				
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB identifies, documents, and implements rules for the acceptable use of information and assets associated with information processing facilities, in accordance with 27001: A.8.1.3.	HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB users ensure that unattended equipment is appropriately protected, in accordance with 27001: A.11.2.8. Both a "clean desk" policy for documents and removable storage media and a "clean screen" policy for information processing services are adopted, in accordance with 27001: A.11.2.9.	HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
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	Shared CSP and CSC	SEEWEB has adopted a policy and supporting security measures to protect information accessed, processed, or stored at remote sites in accordance with 27001: A.6.2.2. Security measures are provided for assets outside the organization's premises, in accordance with 27001: A11.2.6.	HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and	

HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.		HRS-04		Working Policy and Procedures	Human Resources
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	All SEEWEB personnel and users of external parties return the organization's assets in their possession at the end of the period of employment, contract, or agreement entered into, in accordance with		HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated and made effective, in accordance with 27001: A.7.3.		HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Personnel supporting SEEWEB systems and devices must sign a non-disclosure agreement prior to being granted access.		HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Contractual agreements with SEEWEB staff and contractors specify their and the organization's responsibilities with respect to information security, in accordance with 27001: A.7.1.2		HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	SEEWEB has defined and assigned all responsibilities related to information security, in accordance with 27001: A.6.1.1		HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Contractual agreements with SEEWEB staff and contractors specify their and the organization's responsibilities with respect to information security, in accordance with 27001: A.7.1.2. Requirements for NDA agreements for information protection, are identified an reviewed at planned intervals, in		HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	All SEEWEB personnel receive appropriate awareness, education, training and periodic updates on organizational policies and procedures in a manner relevant to their work activities, in accordance with 27001: A.7.2.2.		HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	View response to HRS-11.1.					
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	All SEEWEB personnel receive appropriate awareness, education, training and periodic updates on organizational policies and procedures in a manner relevant to their work activities, in accordance with 27001: A.7.2.2.		HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training	
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	View response to HRS-12.1.					
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	SEEWEB management requires all staff and contractors to apply information security in accordance with the organization's established policies and procedures in accordance with 27001: A.7.2.1.		HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB has defined and documented an access control policy based on business and information security requirements in accordance with 27001: A.9.1.1.		IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.					
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB password policies and guidelines outlines requirements of password strength and handling for passwords used to access internal systems.		IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.					
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	Shared CSP and CSC	In SEEWEB, access to information and functions of application systems is restricted according to access control policies in accordance with 27001: A.9.4.1.	Each customer has his own private Tenant which he can access as an administrator to then be able to manage both users and access levels.	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	

IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and CSC	SEEWEB's conflicting tasks and areas of responsibility are separated to reduce the possibility of misuse of the organization's assets, in accordance with 27001: A.6.1.2.	View response to IAM-03.1
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	The assignment and use of privileged access rights in SEEWEB are limited and controlled, in accordance with 27001: A.9.2.3.	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	SEEWEB has a formal access control policy that is reviewed and updated on an annual basis, in accordance with 27001: A9.	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	Access privilege reviews are triggered from Human Resources. Access privileges are reviewed on an annual basis.	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	SEEWEB asset managers review user access rights at regular intervals, in accordance with 27001: A.9.2.5.	
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	CSP-owned	The assignment and use of privileged access rights in SEEWEB are limited and controlled, in accordance with 27001: A.9.2.3.	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	View response to IAM-09.1.	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	View response to IAM-09.1.	
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	No	CSP-owned		
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Logging of events, user activities, exceptions, malfunctions, and information security events is made and maintained, in accordance with 27001: A.12.4.	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	View response to IAM-12.1.	
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	CSP-owned	SEEWEB implements a formal registration and de-registration process to enable the assignment of access rights, in accordance with 27001: A.9.2.1	
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	Shared CSP and CSC	SEEWEB users are provided only with access to networks and network services for whose use they have been specifically authorized, in accordance with 27001: A.9.1.2. Assignment of secret authentication information is controlled through a formal management process, in accordance with 27001: A.9.2.4. When required by access control policies, access to systems and applications is controlled by secure log-on procedures, in accordance with 27001: A.9.4.2 (i.e. VAULT).	View response to IAM-03.1
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	View response to IAM-14.1.	
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	The assignment of secret authentication information in SEEWEB is controlled through a formal management process in accordance with 27001: A.9.2.4. Users follow the organization's practices, in	

IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	Identity & Access Management
IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	
IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	

IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared CSP and CSC	SEEWEB asset managers review user access rights at regular intervals, in accordance with 27001: A.9.2.5.	View response to IAM-03.1
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	Details regarding SEEWEB APIs can be can be provided upon request.	
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	Details regarding SEEWEB interoperability of each service can be can be provided upon request.	
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Details regarding SEEWEB interoperability of each service can be can be provided upon request.	
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	Details regarding SEEWEB interoperability of each service can be can be provided upon request.	
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned		Details regarding SEEWEB interoperability of each service can be can be provided upon request.
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	SEEWEB APIs and the management console are available via secure, encrypted session using HTTPS, which provide server authentication.	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	SEEWEB customer agreements include data related provisions upon termination. Details regarding contract termination can be found in the customer agreement, see Section 10. https://www.seeweb.it/en/company/terms-and-conditions	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB implements formal, documented policies and procedures that provide guidance for operations and information security within the organization, in accordance with 27001: A.5.	
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	Shared CSP and CSC	Resource utilization is monitored and tuned by SEEWEB in accordance with 27001: A.12.1.3. Projections are made on future capacity requirements to ensure required system performance. Infrastructure monitoring is done	The customer can contractually request the activation of specific monitoring services in addition to reachability.

IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	
IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	

IVS-03.1	Are communications between environments monitored?	Yes	Shared CSP and CSC	Monitoring and alarming are configured to identify and notify operational and management personnel incidents when early warning thresholds are crossed on key operational metrics.		IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	Infrastructure & Virtualization Security
IVS-03.2	Are communications between environments encrypted?	Yes	CSC-owned		SEEWEB APIs and the management console are available via secure, encrypted session using HTTPS, which provide server authentication.				
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	Shared CSP and CSC	SEEWEB's networks are managed and controlled to protect information in systems and applications, according to 27001: A.13.1.1.	APIs and the management console are available via secure,encrypted session using HTTPS, which provide server authentication.				
IVS-03.4	Are network configurations reviewed at least annually?	Yes	Shared CSP and CSC	Regular internal and external vulnerability scans are performed on the host operating system, web application and SEEWEB environment. Vulnerability scanning and remediation practices are regularly reviewed, according to ISO 27001.	Specific security checks are carried out and procedures are manually implemented				
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	Shared CSP and CSC	SEEWEB prohibits all ports and protocols that do not have a specific business purpose, following a rigorous approach to minimal implementation of essential features to use of the device.	The SaaS service only uses protocols and ports authorized by the CSP				
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	Shared CSP and CSC	Changes to SEEWEB's systems are kept under control through the use of formal change control procedures. When changes occur, business-critical applications are reviewed and tested to ensure that there are no adverse impacts on the organization's operational activities or its security, according to 27001: A.14.2.3, A.14.2.4.		IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	SEEWEB's development, test and production environments are separated, according to 27001: A.12.1.4.		IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	In SEEWEB networks, groups of services, users and information systems are segregated according to 27001: A.13.1.3.		IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSC-owned		SEEWEB offers a wide variety of services to help customer migrate data securely.	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	No	CSC-owned			IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	In SEEWEB, information involved in application services transiting over public networks is protected from fraudulent activities, contractual disputes, disclosures, and unauthorized modifications, according to 27001: A.14.1.2.		IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	SEEWEB implements formal, documented policies and procedures that provide guidance for operations and information security within the Organization.		LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.					
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	SEEWEB's logs are protected against loss, destruction, falsification, unauthorized access, and unauthorized release in accordance with 27001: A.18.1.3.		LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSC-owned		The application logs every unauthorized activity	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and	

LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	Shared CSP and CSC	SEEWEB security metrics are monitored and analyzed in accordance with 27001: A.16.	Responsible stakeholders can see logs of security events such as unauthorized requests
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	View response to LOG-02.1.	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	The activities of SEEWEB administrators and system operators are logged, which are protected and reviewed periodically, in accordance with 27001: A.12.4.3.	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	View response to LOG-05.1.	
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	The clocks of all relevant systems processing information within SEEWEB are synchronized with respect to a single reference time source, in accordance with 27001: A.12.4.4.	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	In SEEWEB, logging of events, user activities, exceptions, malfunctions, and information security events is performed and maintained and periodically reviewed, in accordance with 27001: A.12.4.1.	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	View response to LOG-07.1.	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	SEEWEB's log collection facilities and log information are protected from tampering and unauthorized access in accordance with 27001: A.12.4.2.	
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	Shared CSP and CSC	A policy on the use, protection, and durability of cryptographic keys through their entire life cycle has been developed and is implemented in SEEWEB in accordance with 27001: A.12.4.2.	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSC-owned		Application events are logged and stored in a password-protected database
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	CSP-owned	SEEWEB's security areas are protected by appropriate entry controls designed to ensure that only authorized personnel are allowed access, in accordance with 27001: A.11.1.2.	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	Responsibilities and management procedures are established in SEEWEB to ensure rapid, effective and orderly response to information security incidents, in accordance with 27001: A.11.6.1.	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Information security events are reported as quickly as possible through appropriate management channels in accordance with 27001: A.11.6.2.	
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	In SEEWEB responsibilities and management procedures are established to ensure rapid, effective and orderly response to information security incidents in accordance with 27001: A.16.1.1.	
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	In SEEWEB, information security incidents are reported as quickly as possible through appropriate management channels and responded to in accordance with documented procedures, according to 27001: A.16.1.2, A.16.1.5.	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.	

LOG-03		Alerting	Logging and Monitoring
LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	
LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting	
SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	
SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	

SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Information security incidents are responded to in SEEWEB according to documented procedures in accordance with 27001: A.16.1.5.
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	Security incident response plan is tested and policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	Security metrics are monitored and analyzed in SEEWEB in accordance with 27001: A.16.
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	In SEEWEB, safety-related events are evaluated and it is decided whether to classify them as incidents , according to 27001: A.16.1.4.
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	View response to SEF-03.1.
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	View response to SEF-03.1.
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	Appropriate contacts with relevant authorities are maintained in SEEWEB and all contractual requirements, as well as the organization's own approach to meeting them, are defined, documented and kept up-to-date in accordance with 27001:
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	The SSRM policies are established, documented, approved, communicated, applied, evalutated and maintained in SEEWEB (ISMS-DOC-CLD6-3-1).
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	NA	CSP-owned	There are no subcontractors authorized by SEEWEB to access any customer-owned content.
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	NA	CSP-owned	View response to STA-02.1.
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	View response to STA-01.1.
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	View response to STA-01.1.
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	SEEWEB has established a formal audit program that includes continual, independent internal and external assessments.
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	NA	CSP-owned	There are no subcontractors authorized by SEEWEB to access any customer-owned content.
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	NA	CSP-owned	View response to STA-07.1.

SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	
STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	Supply Chain Management, Transparency, and Accountability
STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	

STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	Shared CSP and CSC	SEEWEB service agreements includes multiple provisions and terms. For additional details, see https://www.seeweb.it/en/company/terms-and-conditions
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	SEEWEB's third party agreement processes include periodic review and reporting.
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	CSP-owned	SEEWEB regularly monitors, reviews, and audits service delivery by providers in accordance with 27001: A.15.2.1.
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	SEEWEB's third party agreement processes include periodic review and reporting.
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	NA	CSP-owned	There are no subcontractors authorized by SEEWEB to access any customer-owned content.
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	NA	CSP-owned	View response to STA-13.1.
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	CSP-owned	SEEWEB's information security policies are defined and approved by management, published and communicated to relevant personnel and third parties, are available as documented information, in accordance with 27001: A.5.1.1.
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Detection, prevention, and remediation controls are implemented in SEEWEB with respect to malware, and appropriate user awareness is implemented, in accordance with 27001: A.12.2.1.
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.
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	CSP-owned	View response to TVM-01.1.
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	CSP-owned	SEEWEB's program, processes and procedures to managing antivirus and malicious software is in alignment with ISO 27001 standards.
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	CSP-owned	Rules for the governance of software installation by users have been established and are implemented in SEEWEB in accordance with 27001: A.12.6.2.
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	SEEWEB regularly performs penetration testing and does not share the results directly with customers.
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	SEEWEB regularly performs regular vulnerability scans on the host operating system, web application, and databases in its environment using a variety of tools.

STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	
STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management
TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	
TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	

TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	No	CSP-owned		TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	In SEEWEB, information security events are reported as quickly as possible through appropriate management channels, in accordance with 27001: A.16.1.2.	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	Shared CSP and CSC	SEEWEB tracks metrics for internal process measurements and improvements that align with our policies and standards.	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	SEEWEB has adopted a policy and security measures to support it in managing the risks introduced by the use of portable devices, in accordance with 27001: A.6.2.1.	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	Universal Endpoint Management
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies are reviewed approved by SEEWEB leadership at least annually or as needed basis.				
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	No	CSP-owned		UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Modification of software packages is discouraged and limited to necessary changes, and all changes are strictly controlled, according to 27001: A.14.2.4.	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	The information, other assets associated with information, and information processing facilities of SEEWEB are identified. An inventory of these assets is compiled and kept up-to-date, in accordance with 27001: A.8.1.1.	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	NA	CSP-owned	SEEWEB staff do not access, process, or change customer data in the course of providing our services.	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	SEEWEB has established baseline infrastructure standards in alignment with industry best practices. These include automatic lockout after defined period of inactivity.	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Changes to SEEWEB's systems within the life cycle are kept under control through the use of formal change control procedures in accordance with 27001: A.14.2.2.	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	NA	CSP-owned	View response to UEM-05.1.	UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	View response to UEM-01.1.	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	NA	CSP-owned	Managed endpoints connect to the SEEWEB infrastructure, which is protected by perimeter firewalls.	UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA	CSP-owned	View response to UEM-05.1.	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSP-owned		UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	View response to UEM-01.1.	UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	NA	CSP-owned	View response to UEM-05.1.	UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	
	End of Standard							