A.1 ORGANISATION OF INFORMATION SECURITY

Plan, implement, maintain and continuously improve the information security framework within the organisation

OIS-01 INFORMATION SECURITY MANAGEMENT SYSTEM

Objective

The CSP operates an information security management system (ISMS). The scope of the ISMS covers the CSP's organisational units, locations and processes for providing the cloud service.

Requirements

Ref	Description	Ass. Level
OIS-01.1	The CSP shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes for providing the cloud service	Basic
OIS-01.2	The ISMS shall be in accordance to ISO/IEC 27001	Substantial
OIS-01.3	The ISMS shall have a valid certification according to ISO/IEC 27001 or to national schemes based on ISO 27001	High
OSI-01.4	The CSP shall document the measures for documenting, implementing, maintaining and continuously improving the ISMS	Basic
OIS-01.5	The documentation shall include at least: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).	Substantial

OIS-02 SEGREGATION OF DUTIES

Objective

Conflicting tasks and responsibilities are separated based on an RM-01 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted in the cloud service.

Requirements

Ref	Description	Ass. Level
OIS-02.1	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the cloud service	Basic
OIS-02.2	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the CSP: • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); • Development, testing and release of changes (cf. DEV-01, CCM-01); and • Operation of the system components.	Basic
OIS-02.3	The CSP shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions	Basic

Ref	Description	Ass. Level
OIS-02.4	The CSP shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.	High

OIS-03 CONTACT WITH AUTHORITIES AND INTEREST GROUPS

Objective

The CSP stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks (cf. RM-01) and vulnerabilities (cf. OPS-17).

Requirements

Ref	Description	Ass. Level
OIS-03.1	The CSP shall stay informed about current threats and vulnerabilities	Basic
OIS-03.2	The CSP shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities	Substantial
OIS-03.3	The CSP shall maintain regular contact with its CAB and NCCA to stay informed about current threats and vulnerabilities	High

OIS-04 INFORMATION SECURITY IN PROJECT MANAGEMENT

Objective

Information security is considered in project management, regardless of the nature of the project.

Requirements

Ref	Description	Ass. Level
OIS-04.1	The CSP shall include information security in the project management of all projects that may affect the service, regardless of the nature of the project	Basic
OIS-04.2	The CSP shall perform a risk assessment according to RM-01 to assess and treat the risks on any project that may affect the provision of the cloud service, regardless of the nature of the project	Substantial

A.2 INFORMATION SECURITY POLICIES

Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements

ISP-01 GLOBAL INFORMATION SECURITY POLICY

Objective

The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers.

Requirements

Ref	Description	Ass. Level
ISP-01.1	The CSP shall document a global information security policy covering at least the following aspects: • the importance of information security, based on the requirements of cloud customers in relation to information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the commitment of the CSP to implement the security measures required to achieve the established security objectives. • the most important aspects of the security strategy to achieve the security objectives set; and • the organisational structure for information security in the ISMS application area.	Basic
ISP-01.2	The CSP’s top management shall approve and endorse the global information security policy	Basic
ISP-01.3	The CSP shall review the global information security policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management	Substantial
ISP-01.4	The CSP shall review the global information security policy at least annually	High
ISP-01.5	The CSP shall communicate and make available the global information security policy to internal and external employees and to cloud service customers	Basic

ISP-02 SECURITY POLICIES AND PROCEDURES

Objective

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner.

Requirements

Ref	Description	Ass. Level
ISP-02.1	The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including at least the following aspects: • Objectives; • Scope; • Roles and responsibilities within the organization; • Roles and dependencies on other organisations (especially cloud customers and subservice organisations); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements.	Basic

Ref	Description	Ass. Level
ISP-02.2	The policies and procedures shall include staff qualification requirements and the establishment of substitution rules in their description of roles and responsibilities within the organization	Substantial
ISP-02.3	The CSP shall communicate and make available the policies and procedures to all internal and external employees	Basic
ISP-02.4	The CSP's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies	Basic
ISP-02.5	In case of a delegation, the authorized bodies shall report at least annually to the top management on the security policies and their implementation	High
ISP-02.6	The CSP's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of the cloud service	Basic
ISP-02.7	After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees	Basic

Guidance elements	
ISP-02.1	Add in the guidance the list of requirements that mention policies and procedures, once Annex A is complete.
ISP-02.6	The review of policies and procedures should consider at least the following aspects: • Organisational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the CSP's environment.

ISP-03 EXCEPTIONS

Objective

Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.

Requirements

Ref	Description	Ass. Level
ISP-03.1	The CSP shall maintain a list of exceptions to the security policies and procedures, including associated controls.	Basic
ISP-03.2	The exceptions are limited in time	Basic
ISP-03.3	The exceptions shall be subjected to the RM-01 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners	Substantial
ISP-03.4	The exceptions to a security policy or procedure shall be approved by the top management or authorized body who approved the security policy or procedure	High
ISP-03.5	The list of exceptions shall be reviewed at least annually	Basic
ISP-03.6	The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated	Substantial
ISP-03.7	The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date	High

A.3 RISK MANAGEMENT

Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the CSP

RM-01 RISK MANAGEMENT POLICY

Objective

Risk management policies and procedures are documented and communicated to stakeholders

Reference: [ISO27005]

Requirements

Ref	Description	Ass. Level
RM-01.1	The CSP shall document policies and procedures in accordance with ISP-02 for the following aspects: • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; • Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results.	Basic
RM-01.2	The CSP shall use a documented risk analysis method that guarantees reproducibility and comparability of the approach	Substantial

Guidance elements	
RM-01.2	The notion of “documented method” is close to “standardized method”, but the idea is to allow methods using in a national, vertical or other specific context.

RM-02 RISK ASSESSMENT IMPLEMENTATION

Objective

Risk assessment-related policies and procedures are implemented on the entire perimeter of the cloud service.

Requirements

Ref	Description	Ass. Level
RM-02.1	The CSP shall implement the policies and procedures covering risk assessment on the entire perimeter of the cloud service.	Basic
RM-02.2	The CSP shall make the results of the risk assessment available to relevant stakeholders	Basic
RM-02.3	The CSP shall review and revise the risk assessment at least annually, and after each major change that may affect the security of the cloud service.	Basic
RM-02.4	The CSP shall monitor the evolution of the risk factors and revise the risk assessment results accordingly	High

Guidance elements	
RM-02.1	The scope of risk identification should include the aspects below, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider: • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; • Occurrence of weak points and malfunctions in the integration at system level of technical protective measures; • Attacks via access points, including interfaces accessible from public networks (in particular administrative interfaces); • Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and • Dependencies on subservice organisations.
RM-02.1	For higher assurance levels, specific technical risks should be considered, including: • The risks of failure of the mechanisms of partitioning technical infrastructure resources (memory, calculation, storage, network) that are shared between clients; and • The risks linked to the incomplete or non-secure erasing of data stored in the memory areas or of storage shared between clients, in particular during reallocations of memory and storage areas.

RM-03 RISK TREATMENT IMPLEMENTATION

Objective

Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.

Requirements

Ref	Description	Ass. Level
RM-03.1	The CSP shall prioritize risks according to their criticality	Basic
RM-03.2	The CSP shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them.	Basic
RM-03.3	The risk treatment plan shall reduce the risk level to a threshold that the risk owners deem acceptable (Residual Risk).	Basic
RM-03.4	The risk owners shall formally approve the treatment plan and in particular accept the residual risk	Substantial
RM-03.5	The CSP shall make the risk treatment plan available to relevant stakeholders	Basic
RM-03.6	If the CSP shares risks with the CSC, the shared risks shall be associated to Complementary Customer Controls (CCCs) and described in the user documentation	Basic
RM-03.7	The CSP shall revise the risk treatment plan every time the risk assessment is revised.	Basic
RM-03.8	The risk owners shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.	Substantial

Guidance elements	
RM-03.6	Sharing risks with customers should always be explicit, and associated with clear expectations, typically expressed as CCCs, and included in the documentation (cf. DOC-01).

A.4 HUMAN RESOURCES

Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.

HR-01 HUMAN RESOURCE POLICIES

Objective

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.

Requirements

Ref	Description	Ass. Level
HR-01.1	The CSP shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the cloud service in the production environment, and all positions with access to cloud customer data or system components.	Basic
HR-01.2	The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement from internal and external employees to act ethically in their professional duties.	Basic
HR-01.3	The CSP shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact	Basic
HR-01.4	If disciplinary measures are defined in the policy mentioned in HR-01.3, then the internal and external employees of the CSP shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.	Basic

Guidance elements	
HR-01.2	The agreement should at least stipulate that for any matter related to the security of the cloud service: • professional duties are performed with loyalty, discretion and impartiality; and • Internal and external employees use only those methods, tools and techniques that have been approved by the Cloud Service Provider.
HR-01.2	The Code of Ethics should also consider the following provisions, especially at higher levels: • employees pledge to not disclose information to a third party, even if anonymised and decontextualised, which has been obtained or generated as part of the service, unless the Cloud Service Customer has given formal written authorisation; • employees pledge to alert the service provider to all clearly illegal content discovered during the provision of the service; and • employees pledge to comply with the legislation and regulations in force and with best practices related to their activities.

HR-02 VERIFICATION OF QUALIFICATION AND TRUSTWORTHINESS

Objective

The competency and integrity of all internal and external employees in a position classified in objective HR-01 are verified prior to commencement of employment in accordance with local legislation and regulation by the CSP.

Requirements

Ref	Description	Ass. Level
HR-02.1	The competency and integrity of all internal and external employees of the CSP with access to cloud customer data or system components under the CSP's responsibility, or who are responsible to provide the cloud service in the production environment shall be reviewed before commencement of employment in a position classified in objective HR-01. The extent of the review shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks.	Basic
HR-02.3	The competency and integrity of internal and external employees of the CSP shall be reviewed before commencement of employment in a position with a higher risk classification that their previous position	Substantial
HR-02.4	The competency and integrity of internal and external employees of the CSP shall be reviewed annually for the employees in positions with the highest levels of risk classification, starting at a level to be defined in the human resource policy	High

Guidance elements	
HR-02.1:	The agreement should at least stipulate that for any matter related to the security of the cloud service: • professional duties are performed with loyalty, discretion and impartiality; and • Internal and external employees use only those methods, tools and techniques that have been approved by the CSP. For higher levels, the following areas should also be included: • Request of a police clearance certificate for applicants; and • Evaluation of the risk to be blackmailed.

HR-03 EMPLOYEE TERMS AND CONDITIONS

Objective

The CSP's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the CSP's code of ethics, before being granted access to any cloud customer data or system components under the responsibility of the CSP used to provide the cloud service in the production environment.

Requirements

Ref	Description	Ass. Level
HR-03.1	The CSP shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures	Basic
HR-03.2	The CSP shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	Basic
HR-03.3	The CSP shall give a presentation of all applicable information security policies and procedures to internal and external employees before granting them any access to customer data, the production environment, or any component thereof	Basic
HR-03.4	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof	Substantial

Ref	Description	Ass. Level
HR-03.5	The verification of the acknowledgement defined in HR-03.4 shall be automatically monitored in the processes and automated systems used to grant access rights to employees.	High

HR-04 SECURITY AWARENESS AND TRAINING

Objective

The CSP operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the CSP on a regular basis.

Requirements

Ref	Description	Ass. Level
HR-04.1	The CSP shall define a security awareness and training program that covers the following aspects: • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents.	Basic
HR-04.2	The CSP shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position’s risk classification and technical duties	Substantial
HR-04.3	The CSP shall review their security awareness and training program based on changes to policies and instructions and the current threat situation	Basic
HR-04.4	The CSP shall update their security awareness and training program at least annually	Substantial
HR-04.5	The CSP shall ensure that all employees complete the security awareness and training program defined for them	Basic
HR-04.6	The CSP shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group	Substantial
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program	High
HR-04.8	The CSP shall measure and evaluate the learning outcomes achieved through the awareness and training programme	Substantial
HR-04.9	The CSP shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme.	High
HR-04.10	The CSP shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks	Substantial

HR-05 TERMINATION OR CHANGE IN EMPLOYMENT

Objective

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.

Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.

Requirements

Ref	Description	Ass. Level
HR-05.1	The CSP shall communicate to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed.	Basic
HR-05.2	The CSP shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed	Basic
HR-05.3	The procedure mentioned in HR-05.2 shall define specific roles and responsibilities and include a documented checklist of all required steps	Substantial
HR-05.4	The CSP shall automatically monitor the application of the procedure mentioned in HR-05.2	High

HR-06 CONFIDENTIALITY AGREEMENTS

Objective

Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the CSP to protect the confidentiality of the information exchanged between them.

Requirements

Ref	Description	Ass. Level
HR-06.1	The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers	Basic
HR-06.2	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the CSP for the protection of confidential information and operational details	Substantial
HR-06.3	The agreements shall be accepted by external service providers and suppliers when the contract is agreed	Substantial
HR-06.4	The agreements shall be accepted by internal employees of the CSP before authorisation to access data of cloud customers is granted	Substantial
HR-06.5	The requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly.	Substantial
HR-06.6	The CSP shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.	Substantial
HR-06.7	The CSP shall automatically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers	High

A.5 ASSET MANAGEMENT

Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle

AM-01 ASSET INVENTORY

Objective

The Cloud Service Provider has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.

Requirements

Ref	Description	Ass. Level
AM-01.1	The CSP shall document and implement policies and procedures for maintaining an inventory of assets	Basic
AM-01.2	The inventory shall be performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle	Substantial
AM-01.3	The CSP shall record for each asset the information needed to apply the risk management procedure defined in RM-01.	Basic
AM-01.4	The information recorded with assets shall include the measures taken to manage the risks associated to the asset through its life cycle	Substantial
AM-01.5	The information about assets shall be considered by monitoring applications to identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives, and to support information provided to affected cloud customers in accordance with contractual agreements	High
AM-01.6	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date	High

Guidance elements	
AM-01.1	The assets include the physical and virtual objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility, e.g. firewalls, load balancers, web servers, application servers and database servers.
AM-01.3	The information recorded should include: • the information for identifying the asset • the function of the asset; • the model and version of the asset; • the location of the asset;
AM-01.3	The CSP shall log at least all changes to the information related to risk management on each asset

AM-02 ACCEPTABLE USE AND SAFE HANDLING OF ASSETS POLICY

Objective

Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided in accordance with SP-01, including in particular customer-owned assets and removable media.