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.

Requirements

Ref	Description	Ass. Level
AM-02.1	The CSP shall document, communicate and implement policies and procedures for acceptable use and safe handling of assets (reference to ISP-01)	Basic
AM-02.2	The policies and procedures for acceptable use and safe handling of assets shall address at least the following aspects of the asset lifecycle as applicable to the asset (reference to ISP-01) [list in the guidance]	Substantial
AM-02.3	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use	High

Guidance elements	
AM-02.1	The policies and procedures for acceptable use and safe handling of assets shall address at least the following aspects of the asset lifecycle as applicable to the asset: • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components; • Inventory; • Classification and labelling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support, and security patches are not available anymore; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.
AM-02.3	Definition from NIST's CSRC: Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

AM-03 COMMISSIONING AND DECOMMISSIONING OF HARDWARE

Objective

The Cloud Service Provider has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the cloud service in the production environment, depending on its intended use and based on the applicable policies and procedures.

Requirements

Ref	Description	Ass. Level
AM-03.1	The CSP shall document, communicate and implement a procedure for the commissioning of hardware that is used to provide the cloud service in the production environment, based on applicable policies and procedures	Basic
AM-03.2	The procedure mentioned in AM-03.1 shall ensure that the risks arising from the commissioning are identified, analysed and mitigated.	Substantial

Ref	Description	Ass. Level
AM-03.3	The procedure mentioned in AM-03.1 shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies, before authorization to commission the asset can be granted.	Substantial
AM-03.4	The CSP shall document, communicate and implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, requiring approval based on applicable policies.	Basic
AM-03.5	The procedure mentioned in AM.03-4 shall include the complete and permanent deletion of the data or the proper destruction of the media.	Basic
AM-03.6	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.	High

AM-04 ACCEPTABLE USE, SAFE HANDLING AND RETURN OF ASSETS

Objective

The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service.

Any assets handed over are returned upon termination of employment.

Requirements

Ref	Description	Ass. Level
AM-04.1	The CSP shall ensure and document that all internal and external employees are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-03	Basic
AM-04.2	The procedure mentioned in HR-06.2 shall include steps to ensure that all assets under custody of an employee are returned upon termination of employment.	Basic
AM-04.3	The CSP shall centrally manage the assets under the custody of internal and external employees, including at least software, data, and policy distribution, as well as remote deactivation, deletion or locking, as available on the asset.	High
AM-04.4	The verification of the commitment defined in AM-04.1 shall be automatically monitored	High

AM-05 ASSET CLASSIFICATION AND LABELLING

Objective

Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.

Requirements

Ref	Description	Ass. Level
AM-05.1	The CSP shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits	Basic

Ref	Description	Ass. Level
AM-05.2	The asset classification schema shall provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives	Substantial
AM-05.3	When applicable, the CSP shall label all assets according to their classification in the asset classification schema	Basic
AM-05.4	The need for protection shall be determined by the individuals or groups responsible for the assets	Substantial

Guidance elements	
AM-05.3	Definition of a label: “The means used to associate a set of security attributes with an asset”. Note that labelling is not necessarily physical.

A.6 PHYSICAL SECURITY

Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations

PS-01 PHYSICAL SECURITY PERIMETERS

Objective

The buildings and premises related to the cloud service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises.

Requirements

Ref	Description	Ass. Level
PS-01.1	The CSP shall define security perimeters in the buildings and premises related to the cloud service provided	Basic
PS-01.2	The CSP shall define at least two security areas, with one covering all buildings and premises and one covering sensitive activities such as the buildings and premises hosting the information system for the production of the service	Basic
PS01-3	The CSP shall define at least an additional private area that may host development activities and administration, supervision and operation workstations	High
PS-01.4	The CSP shall ensure that no direct access exists between a public area and a sensitive area	High
PS-01.5	The CSP shall ensure that all delivery, loading areas, and other points through which unauthorised persons can penetrate into the premises without being accompanied are part of the public area	High
PS-01.6	The CSP shall define and communicate a set of security requirements for each security area in a policy according to SP-02	Basic
PS-01.7	The security requirements in PS-01.5 shall be based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security	Substantial

PS-02 PHYSICAL SITE ACCESS CONTROL

Objective

Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.

Requirements

Ref	Description	Ass. Level
PS-02.1	The CSP shall document, communicate and implement policies and procedures related to the physical access control to the security areas matching the requirements defined in PS-01 and based on the principles defined in IAM-01	Basic
PS-02.2	The access control policy shall require at least one authentication factor for accessing any non-public area	Basic
PS-02.3	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process cloud customer data	Substantial

Ref	Description	Ass. Level
PS-02.4	The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay	Substantial
PS-02.5	The access control policy shall describe the physical access control derogations in case of emergency	Basic
PS-02.6	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users	High
PS-02.7	The CSP shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters	Basic
PS-02.8	The CSP shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner so that it does not compromise the information security of the cloud service	Basic
PS-02.9	The access control policy shall include logging of all accesses to non-public areas that enables the CSP to check whether only defined personnel have entered these zones	Substantial
PS-02.10	The logging of accesses shall be automatically monitored to guarantee fulfilment of PS-02.9	High

Guidance elements	
PS-02.4	Third-party personnel do not include external employees, who are subject to HR policies and do not have to be supervised
PS-02.8	A mix of prevention and detection measures are possible, and “timely” will be defined in greater details in the guidance for the different assurance levels and areas

PS-03 WORKING IN NON-PUBLIC AREAS

Objective

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.

Requirements

Ref	Description	Ass. Level
PS-03.1	The CSP shall document, communicate, and implement policies and procedures concerning work in non-public areas	Basic
PS-03.2	The policies and procedures in PS-02.1 shall include a clear screen policy and a clear desk policy for documents and removable media	Substantial
PS-03.3	The CSP shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area	High
PS-03.4	The CSP shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area	High

PS-04 EQUIPMENT PROTECTION

Objective

The equipment used in the Cloud Service Provider's premises and buildings are protected physically against damage and unauthorized access by specific measures.

Requirements

Ref	Description	Ass. Level
PS-04.1	The CSP shall document, communicate, and implement policies and procedures concerning the protection of equipment and including at least the following aspects: • Protecting power and communications cabling from interception, interference or damage; • Protecting equipment during maintenance operations; • Protecting equipment holding customer data during transport.	Basic
PS-04.2	The procedures defined in PS-04.1 shall include a procedure to check the protection of power and communications cabling, to be performed regularly, at least every two years, as well as in case of suspected manipulation by qualified personnel	Substantial
PS-04.3	The policies and procedures in PS-04.1 shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site	Substantial
PS-04.4	The procedure mentioned in PS-04.3 shall include a formal validation by top management of the CSP or by the authorized body that validated this procedure	High
PS-04.4	The CSP shall establish a wiring scheme and keep it up-to-date	High
PS-04.5	The CSP shall ensure that the maintenance agreements for equipment used to host the cloud service make it possible to have security updates installed timely on this equipment	High
PS-04.6	The policies and procedures in PS-04.1 shall include measures to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) are compatible with the cloud service's availability and security requirements	High
PS-04.7	The CSP shall ensure that an equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted in accordance with CKM-03 or has been destroyed beforehand using a secure deletion mechanism	High
PS-04.8	The CSP shall use encryption on the removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media	Basic

Guidance elements	
PS-04.2	The checks to be performed should include at least the following aspects: • Traces of violent attempts to open closed distributors; • Up-to-datedness of the documentation in the distribution list; • Conformity of the actual wiring and patching with the documentation; • The short-circuits and earthing of unneeded cables are intact; and • Impermissible installations and modifications.

PS-05 PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

Objective

The premises from which the cloud service operated, and in particular its data centres, are protected against external and environmental threats.

Requirements

Ref	Description	Ass. Level
PS-05.1	The CSP shall document and communicate a set of security requirements related to external and environmental threats in a policy according to SP-02, addressing the following risks in accordance with the applicable legal and contractual requirements: • Faults in planning; • Unauthorised access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration.	Basic
PS-05.2	The security requirements defined in PS-05.1 for datacentres shall be based on criteria which comply with established rules of technology	Substantial
PS-05.3	The security requirements defined in PS-05.1 for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime	High
PS-05.4	The security requirements defined in PS-05.1 for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually	High
PS-05.5	The CSP shall provide the cloud service from at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience	Substantial
PS-05.6	The CSP shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises (cf. BCM-04)	Substantial

Guidance elements	
PS-05.2	The “established rules of technology” will be refined in guidance
PS-05.5	There are cloud providers who no longer address the issue of reliability of the cloud service on a physical level through redundancy from two independent locations, but through resilience. The cloud service is provided simultaneously from more than two locations. The underlying distributed data centre architecture ensures that the failure of a location or components of a location does not violate the defined availability criteria of the cloud service.

A.7 OPERATIONAL SECURITY

Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures

OPS-01 CAPACITY MANAGEMENT – PLANNING

Objective

The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.

Requirements

Ref	Description	Ass. Level
OPS-01.1	The CSP shall document and implement procedures to plan for capacities and resources (personnel and IT resources), which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload	Basic
OPS-01.2	The CSP shall meet the requirements included in contractual agreements with cloud customers regarding the provision of the cloud service in case of capacity bottlenecks or personnel and IT resources outages	Basic
OPS-01.3	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning	High

OPS-02 CAPACITY MANAGEMENT – MONITORING

Objective

The capacities of critical resources such as personnel and IT resources are monitored.

Requirements

Ref	Description	Ass. Level
OPS-02.1	The CSP shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning of cloud services to ensure compliance with the service level agreement	Basic
OPS-02.2	The CSP shall make available to the cloud customer the relevant information regarding capacity and availability on a self-service portal	High
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1	High

OPS-03 CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES

Objective

The CSCs have the ability to manage the IT resources allocated to them in order to avoid overcrowding of resources and to achieve sufficient performance.

Requirements

Ref	Description	Ass. Level
OPS-03.1	The CSP shall enable CSCs to control and monitor the allocation of the system resources assigned to them, if the corresponding cloud capabilities are exposed to the CSCs	Basic

OPS-04 PROTECTION AGAINST MALWARE – POLICIES

Objective

Policies are defined that ensure the protection against malware of IT equipment related to the cloud service.

Requirements

Ref	Description	Ass. Level
OPS-04.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects: • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.	Basic
OPS-04.2	The CSP shall create regular reports on the malware checks performed, which shall be reviewed and analysed by authorized bodies in the reviews of the policies related to malware	Substantial
OPS-04.3	The policies and instructions related to malware shall include the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces (both the customer's self-service and the CSP's administration)	High
OPS-04.4	The CSP shall update the anti-malware products at the highest frequency that the vendors actually offer	High

OPS-05 PROTECTION AGAINST MALWARE – IMPLEMENTATION

Objective

Malware protection is deployed and maintained on systems that provide the cloud service.

Requirements

Ref	Description	Ass. Level
OPS-05.1	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the production environment, according to policies and procedures	Basic
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial
OPS-05.3	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of OPS-05.1	High
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	High

Guidance elements	
OPS-05.1	The locution “if technically feasible” refers to the fact that some equipment cannot be equipped with specific malware protection (typically, embedded systems).

OPS-06 DATA BACKUP AND RECOVERY – POLICIES

Objective

Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.

Requirements

Ref	Description	Ass. Level
OPS-06.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery	Basic
OPS-06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08).	Substantial

OPS-07 DATA BACKUP AND RECOVERY – MONITORING

Objective

The proper execution of data backups is monitored.

Requirements

Ref	Description	Ass. Level
OPS-07.1	The CSP shall document and implement technical and organizational measures to monitor the execution of data backups in accordance to the policies and procedures defined in OPS-06	Basic
OPS-07.2	The CSP shall make available to its customers a self-service portal for automatically monitoring their data backup to guarantee fulfilment with OPS-07.1	High
OPS-07.3	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1	High

OPS-08 DATA BACKUP AND RECOVERY – REGULAR TESTING

Objective

The proper restoration of data backups is regularly tested.

Requirements

Ref	Description	Ass. Level
OPS-08.1	The CSP shall test the restore procedures at least annually	Basic
OPS-08.2	The restore tests shall assess if the specifications for the RTO and RPO agreed with the customers are met	Substantial
OPS-08.3	Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation	Substantial
OPS-08.4	The CSP shall inform CSCs, at their request, of the results of the recovery tests	High
OPS-08.5	Recovery tests shall be included in the CSP's business continuity management	High

OPS-09 DATA BACKUP AND RECOVERY – STORAGE

Objective

Backup data is stored at an appropriately remote location.

Requirements

Ref	Description	Ass. Level
OPS-09.1	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location	Basic
OPS-09.2	When the backup data is transmitted to a remote location via a network, the transmission of the data takes place in an encrypted form that corresponds to the sate-of-the-art (cf. CKM-02).	Basic
OPS-09.3	The CSP shall select a remote location to store its backups concerning the distance, recovery times and the impact of disasters of both sites	Substantial
OPS-09.4	The physical and environmental security measures at the remote site shall have the same level as at the main site	Substantial
OPS-09.5	When the backup data is transmitted to a remote location via a network, the CSP shall automatically monitor the transmission to guarantee fulfilment of OPS-09.1	High

OPS-10 LOGGING AND MONITORING – POLICIES

Objective

Policies are defined to govern logging and monitoring events on system components under the CSP's responsibility.

Requirements

Ref	Description	Ass. Level
OPS-10.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility	Basic
OPS-10.2	The policies and procedures shall cover at least the following aspects:	Substantial

Ref	Description	Ass. Level
	• Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs; • Define roles and responsibilities for setting up and monitoring logging; • Time synchronisation of system components; and • Compliance with legal and regulatory frameworks.	

OPS-11 LOGGING AND MONITORING – DERIVED DATA MANAGEMENT

Objective

Policies are defined to govern the management of derived data by the CSP.

Requirements

Ref	Description	Ass. Level
OPS-11.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 that govern the secure handling of derived data	Basic
OPS-11.2	The policies and procedures on derived data shall cover at least the following aspects: • Purpose for the collection and use of derived data beyond the operation of the cloud service, including purposes related to the implementation of security controls; • Anonymisation of the data whenever used in a context that goes beyond a single CSC; • Period of storage reasonably related to the purposes of the collection; • Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and • Provision of the derived data to CSCs according to contractual agreements.	Substantial
OPS-11.3	The CSP shall list in the contractual agreement with the CSC all purposes for the collection of use of derived data that are not related to the implementation of security controls or to billing	Substantial
OPS-11.4	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.	High

Guidance elements	
Terminology	Derived data is defined as “data under cloud service provider control that is derived as a result of interaction with the cloud service by the CSC”. It obviously includes logging and monitoring data, but not only. The idea in this subcategory is to ensure that declarations from the CSP are complete
OPS-11.2	Most derived data has a transient use in the operation of the cloud service, the focus is here on derived data collected by the CSP

OPS-12 LOGGING AND MONITORING – IDENTIFICATION OF EVENTS

Objective

Logs are monitored to identify events that may lead to security incidents.

Requirements

Ref	Description	Ass. Level
OPS-12.1	The CSP shall monitor log data in order to identify events that might lead to security incidents, in accordance with the logging and monitoring requirements	Basic
OPS-12.2	Identified events shall be reported to the appropriate departments for timely assessment and remediation.	Basic
OPS-12.3	The monitoring of events mentioned in OPS-12.1 shall be automated	Substantial
OPS-12.4	The CSP shall automatically monitor that event detection is effective on the list of critical assets in fulfilment of OPS-12.1	High

OPS-13 LOGGING AND MONITORING – ACCESS, STORAGE AND DELETION

Objective

The confidentiality, integrity and availability of logging and monitoring data are protected with measures adapted to their specific use.

Requirements

Ref	Description	Ass. Level
OPS-13.1	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation	Basic
OPS-13.2	Log data shall be deleted when it is no longer required for the purpose for which they were collected	Basic
OPS-13.3	The communication between the assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality	Basic
OPS-13.4	The communication between the assets to be logged and the logging servers shall be encrypted using state-of-the-art encryption or shall take place on a dedicated administration network	Substantial
OPS-12.5	The CSP shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: • Access only to authorised users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	Substantial
OPS-13.6	The CSP shall provide CSCs, upon request, access to customer-specific logging through an API. The logging shall comply with the CSP's protection requirements, including logical or physical separation of log and customer data	High
OPS-13.7	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2	High

Guidance elements	
OPS-13.6	From C5, the customer-specific logging may be specific "in terms of scope and duration of the retention period"

OPS-14 LOGGING AND MONITORING – ATTRIBUTION

Objective

Log data can be unambiguously attributed to a CSC.

Requirements

Ref	Description	Ass. Level
OPS-14.1	The log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis in the event of an incident	Basic
OPS-14.2	The CSP shall make available interfaces to conduct forensic analysis and perform backups of infrastructure components and their network communication	Substantial
OPS-14.3	In the context of an investigation of an incident concerning a CSC, the CSP shall have the ability to provide to the CSC the logs related to its cloud service	High

Guidance elements	
OPS-14.3	Guidance should be provided to indicate that local regulations related to investigations should guide the way in which these logs should be made available

OPS-15 LOGGING AND MONITORING – CONFIGURATION

Objective

Access to the logging and monitoring system components and to their configuration is strictly restricted.

Requirements

Ref	Description	Ass. Level
OPS-15.1	The CSP shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility	Basic
OPS-15.2	Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01)	Basic
OPS-15.3	The access to system components for logging and monitoring shall require strong authentication	Substantial

OPS-16 LOGGING AND MONITORING – AVAILABILITY

Objective

Systems for logging and monitoring are themselves monitored for availability.

Requirements

Ref	Description	Ass. Level
OPS-16.1	The CSP shall monitor the system components for logging and monitoring under its responsibility, and shall automatically report failures to the responsible departments for assessment and remediation	Basic

Ref	Description	Ass. Level
OPS-16.2	The CSP shall design the system components for logging and monitoring in such a way that the overall functionality is not restricted if individual components fail	High

OPS-17 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES

Objective

Vulnerabilities in the system components used to provide the cloud service are identified and addressed in a timely manner.

Requirements

Ref	Description	Ass. Level
OPS-17.1	The CSP shall document, communicated and implement in accordance to ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service	Basic
OPS-17.2	The policies and procedures shall describe measures regarding at least the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	Substantial
OPS-17.3	The CSP shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities	Basic
OPS-17.4	The CSP shall mandate in its policies and procedures the immediate handling of “critical” vulnerabilities and the handling of “high” vulnerabilities within a day, with a follow-up of the vulnerability until it has been remediated	Substantial

Guidance elements	
OPS-17.3	The requirement stops short of requiring the use of CVSS, although the CSP is encouraged to use a version of CVSS. As a rule of thumb: • A critical vulnerability would correspond to CVSS scores between 9.0 and 10.0 • A high vulnerability would correspond to CVSS scores between 7.0 and 8.9
OPS-17.4	A critical vulnerability is expected to be handled within a few hours, and the EUCS scheme requires the CSP to notify its CAB of such a vulnerability.

OPS-18 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – ONLINE REGISTERS

Objective

Online registers are used to identify and publish known vulnerabilities.

Requirements

Ref	Description	Ass. Level
OPS-18.1	The CSP shall publish and maintain a publicly and easily accessible online register of known vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or operate under their own responsibility	Basic
OPS-18.2	The online register shall indicate at least the following information for every vulnerability: • A presentation of the vulnerability following an industry-accepted scoring system; • A description of the remediation options for that vulnerability; • Information on the availability of updates or patches for that vulnerability; • Information about the remediation or deployment of patches or updates by the CSP or CSC, including detailed instructions for operations to be performed by the CSC.	Basic
OPS-18.3	The CSP shall publish and maintain a list of pointers to online registers published by its subservice providers and suppliers, or integrate regularly the content of these online registers relevant to the cloud service into its own online register (cf. OPS-18.1)	Basic
OPS-18.4	The CSP shall consult regularly the online registers published by its subservice providers and suppliers, analyse the potential impact of the published vulnerabilities on the cloud service, and handle them according to the vulnerability handling process (cf. OPS-17)	Basic
OPS-18.5	The CSP shall consult the online registers published by its subservice providers and suppliers at least daily, and update accordingly its own online register	Substantial
OPS-18.6	The CSP shall equip with automatic update mechanisms the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC	High

Guidance elements	
OPS-18.2	The Common Vulnerability Scoring System (CVSS) should be used.

OPS-19 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – VULNERABILITY IDENTIFICATION

Objective

Tests are performed on a regular basis to identify vulnerabilities.

Requirements

Ref	Description	Ass. Level
OPS-19.1	The CSP shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the cloud service, in accordance with policies for handling vulnerabilities (cf. OPS-17)	Basic
OPS-19.2	The CSP shall perform the tests defined in OPS-18.1 at least once a month	Substantial
OPS-19.2	The CSP shall have penetration tests carried out by qualified internal personnel or external service providers, according to a documented test methodology and including in their scope the system components relevant to the provision of the cloud service in the area of responsibility of the CSP, as identified in a risk analysis	Substantial
OPS-19.3	The CSP shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures (cf. OPS-18).	Substantial

Ref	Description	Ass. Level
OPS-19.4	The tests are performed following a multi-annual work program, reviewed annually, that covers system components and security controls according to the evolution of the cloud service and of the threat landscape.	High
OPS-19.5	Some of the penetration tests performed each year shall be performed by external service providers	High
OPS-19.6	The CSP shall perform a root cause analysis on the vulnerabilities discovered through penetration testing in order to assess to which extent similar vulnerabilities may be present in the cloud system	High
OPS-19.7	The CSP shall correlate the possible exploits of discovered vulnerabilities with previous incidents to identify if the vulnerability may have been exploited before its discovery	High

Guidance elements	
OPS-19.1	This requirement has been added in order to match the level expected for Basic. Guidance will explain that automated testing will be acceptable at the Basic level.
OPS-19.2	The required qualifications will be further defined in guidance, and they should include some kind of personal of service certification
OPS-19.4	The idea is here that the CAB shall review the penetration testing plan and to identify nonconformities to be fixed (i.e., tests that are missing and may need to be included and performed in the following years), following procedures to be defined in guidance for auditors
OPS-19.5	The idea is also here to use the program to ensure that if there is an internal team, they use external providers to ensure that their competencies remain adequate, and to learn new things.
OPS-19.7	At this level, the CSP needs to ask the question of the potential exploitation of the vulnerability in the past, by determining potential symptoms of exploitation and searching for them in logs.

OPS-20 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – MEASUREMENTS, ANALYSES AND ASSESSMENTS OF PROCEDURES

Objective

The vulnerability and incident handling measures are regularly evaluated and improved.

Requirements

Ref	Description	Ass. Level
OPS-20.1	The CSP shall regularly measure, analyse and assess the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness	Basic
OPS-20.2	The CSP shall organize a quarterly review of the results of the assessment defined in OPS-20.1 by accountable departments to initiate continuous improvement actions and verify their effectiveness	Substantial

OPS-21 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – SYSTEM HARDENING

Objective

System components are hardened to reduce their attack surface and eliminate potential attack vectors.

Requirements

Ref	Description	Ass. Level
OPS-21.1	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards	Basic
OPS-21.2	The hardening requirements for each system component shall be documented	Basic
OPS-21.3	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications	High

Guidance elements	
OPS-21.1	If the CSP is using non-modifiable images, the hardening process should be done during the creation of those images. Configuration and log files regarding the continuous availability of the images should be retained

OPS-22 SEPARATION OF DATASETS IN THE CLOUD INFRASTRUCTURE

Objective

System components are hardened to reduce their attack surface and eliminate potential attack vectors.

Requirements

Ref	Description	Ass. Level
OPS-21.1	The CSP shall segregate the CSC data stored and processed on shared virtual and physical resources to ensure the confidentiality and integrity of this data, according to the results of a risk analysis (cf. RM-01)	Basic

A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT

Limit access to information and information processing facilities

IAM-01 POLICIES FOR ACCESS CONTROL TO INFORMATION

Objective

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.

Requirements

Ref	Description	Ass. Level
IAM-01.1	The CSP shall document, communicate and make available role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on the business and security requirements of the CSP, in which at least the following aspects are covered: • Parameters to be considered for making access control decisions • Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle. • Use of a role-based mechanism for the assignment of access rights • Segregation of duties between managing, approving and assigning access rights • Dedicated rules for users with privileged access • Requirements for the approval and documentation of the management of access rights	Basic
IAM-01.2	The CSP shall link the access control policy defined in IAM-01.1 with the physical access control policy defined in PS-02.1, to guarantee that the access to the premises where information is located is also controlled.	Basic
IAM-01.3	The CSP shall base its access control policy on the use of role-based access control.	Substantial

IAM-02 MANAGEMENT OF USER ACCOUNTS

Objective

Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.

Requirements

Ref	Description	Ass. Level
IAM-02.1	The CSP shall document policies for managing accounts, according to ISP-02, in which at least the following aspects are described: • Assignment of unique usernames • Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type • Events leading to blocking and revoking accounts	Basic
IAM-02.2	The CSP shall document, communicate and make available policies for managing accounts of users under the responsibility of the CSP, according to ISP-02 and extending the policies defined in IAM-02.1, in which at least the following aspects are described: • Segregation of duties between managing, approving and assigning user accounts • Regular review of assigned user accounts and associated access rights	Substantial

Ref	Description	Ass. Level
	• Blocking and revoking accounts in the event of inactivity or potential account compromise • Requirements for the approval and documentation of the management of user accounts	
IAM-02.3	The CSP shall document, communicate and make available policies for managing accounts of users under the responsibility of the CSCs, according to ISP-02 and extending the policies defined in IAM-02.1, in which at least the following aspects are described: • Access control mechanisms available to CSCs • Access control parameters that the CSC is allowed to configure	Substantial
IAM-02.4	The CSP shall document and implement procedures for managing personal user accounts and access rights to internal and external employees that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.5	The CSP shall document and implement procedures for managing non-personal shared accounts and associated access rights that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.6	The CSP shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.7	The CSP shall offer CSCs a self-service with which they can independently manage user accounts for all users under their responsibility.	Substantial
IAM-02.8	The CSP shall be able to provide, for a given user account, whether it falls under the responsibility of the CSP or of the CSC, as well as the list of the access rights granted to that account.	High

IAM-03 LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS

Objective

Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.

Requirements

Ref	Description	Ass. Level
IAM-03.1	The CSP shall define and implement an automated mechanism to block user accounts after a certain period of time	Basic
IAM-03.2	The automated mechanism in IAM-03.1 shall block personal user accounts under the responsibility of the CSP after two (2) months of inactivity.	Substantial
IAM-03.3	The CSP shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts	Basic
IAM-03.4	The limits on authentication attempts used in mechanism IAM-03.3 for user accounts under the responsibility of the CSP shall be based on the risks on the accounts, associated access rights and authentication mechanisms	Substantial
IAM-03.5	The CSP shall document a process to monitor stolen and compromised credentials and lock any pending account for which an issue is identified, pending a review by an authorized person	Substantial
IAM-03.6	The CSP shall implement the process in IAM-03.5 on all user accounts under its responsibility to which privileged access rights are assigned	Substantial

Ref	Description	Ass. Level
IAM-03.7	The CSP shall implement the process in IAM-03.5 on all user accounts under its responsibility	High
IAM-03.8	Approval from authorised personnel or system components is required to unlock accounts locked automatically	Substantial
IAM-03.9	The CSP shall define and implement an automated mechanism to revoke user accounts that have been blocked by another automatic mechanism after a certain period of time	Substantial
IAM-03.10	The automated mechanism in IAM-03.9 shall revoke user accounts under the responsibility of the CSP after they have been blocked for six (6) months.	Substantial
IAM-03.11	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03	High
IAM-03.12	The CSP shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons	High

IAM-04 MANAGEMENT OF ACCESS RIGHTS

Objective

Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.

Requirements

Ref	Description	Ass. Level
IAM-04.1	The CSP shall document and implement procedures to grant, update, and revoke to a user account under its responsibility access rights to resources of the information system of the cloud service, and these procedures shall be compliant with the role and rights concept and with the policies for managing access rights	Basic
IAM-04.2	The CSP shall document and implement a procedure to timely update or revoke the access rights of an internal or external employee when the role and responsibilities of the employee change.	Basic
IAM-04.3	The update or revocation of access rights procedure defined in IAM-04.2 shall be executed within 48 hours of the role change for privileged access rights and within 14 days for other access rights.	Substantial
IAM-04.4	The CSP shall document a procedure to provide, for a given resource subject to access control the list of all the user accounts that have access to it, whether they fall under the responsibility of the CSP or of a CSC, and for every such account the list of access rights currently granted to it	High
IAM-04.5	The CSP shall document the incompatibility between access rights, and enforce these incompatibilities when access rights are granted or updated on a user account	High
IAM-04.6	The access right management procedures shall follow a dynamic approach	High
IAM-04.7	The CSP shall offer CSCs a self-service with which they can independently manage access rights for all user accounts under their responsibility.	Substantial

Guidance elements	
IAM-04.6	The 'dynamic approach' implies that the modification of access rights takes effect immediately, without requiring the user to logout and log back in (unless new access rights have been granted that require a more stringent authentication method)

IAM-05 REGULAR REVIEW OF ACCESS RIGHTS

Objective

The fitness for purpose of the user accounts of all types and their associated access rights are reviewed regularly.

Requirements

Ref	Description	Ass. Level
IAM-05.1	The CSP shall review the access rights of all the user accounts under its responsibility at least once a year to ensure that they still correspond to the current needs	Basic
IAM-05.2	The review defined in IAM-05.1 shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies.	Substantial
IAM-05.3	The CSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights.	Substantial
IAM-05.4	The CSP shall provide CSCs with a tool that facilitates the review of the access rights of user accounts under their responsibility	Substantial
IAM-05.5	The CSP shall perform the review defined in IAM-05.1 at least every six (6) months	High

IAM-06 PRIVILEGED ACCESS RIGHTS

Objective

Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.

Requirements

Ref	Description	Ass. Level
IAM-06.1	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks (need-to-know principle)	Substantial
IAM-06.2	Activities of users with privileged access rights shall be logged in order to detect any misuse of privileged access or function in suspicious cases, and the logged information shall be automatically monitored for defined events that may indicate misuse	Substantial
IAM-06.3	The CSP shall document and implement a procedure that, upon detection of potential misuse by the monitoring defined in IAM-06.2, informs the responsible personnel so that they can promptly assess whether misuse has occurred and take corresponding action.	Substantial
IAM-06.4	Shared accounts under the responsibility of the CSP shall be assigned only to internal or external employees	Basic
IAM-06.5	The CSP must revise every three (3) months the list of employees who are responsible for a technical account within its scope of responsibility	High

Ref	Description	Ass. Level
IAM-06.6	The CSP shall maintain an up-to-date inventory of the user accounts under its responsibility that have privileged access rights	High
IAM-06.7	The CSP shall require strong authentication for accessing the administration interfaces used by the CSP	Substantial
IAM-06.8	The CSP shall require strong authentication for accessing the administration interfaces offered to the CSC	High

Guidance elements	
IAM-06.4	Shared account are typically privileged; they should also be assigned to more than one employee
IAM-06.7 IAM-06.8	The notion of “strong authentication” will need to be described in the guidance, along the lines of: • for human users, two-factor or multi-factor authentication; and • for non-human users, authentication using a cryptographic mechanism that satisfies the requirements in CKM-01.

IAM-07 AUTHENTICATION MECHANISMS

Objective

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.

Requirements

Ref	Description	Ass. Level
IAM-07.1	The CSP shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: • The selection of mechanisms suitable for every type of account and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new accounts; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules;	Basic
IAM-07.2	The access to all environments of the CSP shall be authenticated, including non-production environments	Substantial
IAM-07.3	The access to the production environment of the CSP shall require strong authentication	High
IAM-07.4	The access to all environments of the CSP containing CSC data shall require strong authentication	High
IAM-07.5	Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security	Substantial
IAM-07.6	For access to non-personal shared accounts, the CSP shall implement measures that require the users to be authenticated with their personal account before being able to access these technical accounts	Substantial
IAM-07.7	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts	Basic

Ref	Description	Ass. Level
IAM-07.8	The CSP shall offer strong authentication methods to the CSC for use with the accounts under their responsibility	Substantial

IAM-08 PROTECTION AND STRENGTH OF CREDENTIALS

Objective

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.

Requirements

Ref	Description	Ass. Level
IAM-08.1	The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: • Non-reuse of credentials • Trade-offs between entropy and ability to memorize • Recommendations for renewal of passwords • Rules on storage of passwords	Basic
IAM-08.2	The CSP rules and recommendations defined in IAM-08.1 shall address at least the following aspects: • Recommendations on password managers • Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling	Substantial
IAM-08.3	The CSP shall require users to whom authentication credentials are provided to sign a declaration in which they assure that they treat personal (or shared) authentication confidentially and keep it exclusively for themselves	High
IAM-08.4	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01)	Basic
IAM-08.5	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	Basic
IAM-08.6	When creating credentials, compliance with specifications is enforced automatically as far as technically possible	Substantial
IAM-08.7	When a credential associated to a personal account is changed or renewed, the person associated to that account shall be notified	Substantial
IAM-08.8	Any password communicated to a user through e-mail, message or similar shall be changed by the user after its first use, and its validity shall not exceed 14 days after communication to the user	Substantial
IAM-08.9	The CSP shall make available to the CSC the rules and recommendations that shall or may apply to the users under their responsibility, and provide the CSC with tools to manage and enforce these rules	Substantial

IAM-09 GENERAL ACCESS RESTRICTIONS

Objective

The assets in and around the cloud service are managed in a way that ensure that access restrictions are enforced between different categories of assets.

Requirements

Ref	Description	Ass. Level
IAM-09.1	The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems	Basic
IAM-09.2	The CSP shall design, develop, configure and deploy the information system providing the cloud service to include a partitioning between the technical infrastructure and the equipment required for the administration of the cloud service and the assets it hosts	Substantial
IAM-09.3	The CSP shall separate the administration interfaces made available to CSCs from those made available to its internal and external employees, and in particular: • The administration accounts under the responsibility of the CSP shall be managed using tools and directories that are separate from those used for the management of user accounts under the responsibility of the CSCs; • The administration interfaces made available to CSCs shall not allow for any connection from accounts under the responsibility of the CSP; • The administration interfaces used by the CSP shall not be accessible from the public network and as such shall not allow for any connection from accounts under the responsibility of the CSC.	High
IAM-09.4	The CSP shall implement suitable measures for partitioning between the CSCs	Basic
IAM-09.5	The CSP shall timely inform a CSC whenever internal or external employees of the CSP access in a non-encrypted form to the CSC's data processed, stored or transmitted in the cloud service without the prior consent of the CSC, including at least: • Cause, time, duration, type and scope of the access; • Enough details to enable subject matters experts of the CSC to assess the risks of the access.	Substantial
IAM-09.6	The CSP shall require prior consent from a CSC before any access in a non-encrypted form to the CSC's data processed, stored or transmitted in the cloud service, providing meaningful information as defined in IAM-09.5.	High
IAM-09.7	If the CSP offers to its CSCs interfaces for administrators and for end users, these interfaces shall be separated	Substantial

Guidance elements	
IAM-09.1	This does not preclude connections between the provision of the cloud service and other information systems, for instance for billing purposes or for backup purposes, but such purposes should be clearly identified and the interfaces clearly defined.

A.9 CRYPTOGRAPHY AND KEY MANAGEMENT

Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information

CKM-01 POLICIES FOR THE USE OF ENCRYPTION MECHANISMS AND KEY MANAGEMENT

Objective

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.

Requirements

Ref	Description	Ass. Level
CKM-01.1	The CSP shall document, communicate, make available and implement policies with technical and organizational safeguards for encryption and key management, according to ISP-02, in which at least the following aspects are described: • Usage of strong encryption procedures and secure network protocols • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys • Consideration of relevant legal and regulatory obligations and requirements	Basic
CKM-01.2	Cryptography policies and procedures shall include risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption	Substantial
CKM-01.3	The strong encryption procedures and secure network protocols mentioned in the cryptography policies and procedures shall correspond to the state-of-the-art	Substantial

Guidance elements	
CKM-01.3	The notion of “state-of-the-art” will need to be defined, together with references to external guides, if possible European

CKM-02 ENCRYPTION OF DATA IN TRANSIT

Objective

Cloud customer data communicated over public networks is protected in confidentiality, integrity, and authenticity.

Requirements

Ref	Description	Ass. Level
CKM-02.1	The CSP shall define and implement strong encryption mechanisms for the transmission of cloud customer data over public networks	Basic
CKM-02.2	The CSP shall define, and implement strong encryption mechanisms for the transmission of all data over public networks	High

CKM-03 ENCRYPTION OF DATA AT REST

Objective

The CSP has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage.

Requirements

Ref	Description	Ass. Level
CKM-03.1	The CSP shall document and implement procedures and technical safeguards to encrypt cloud customers' data during storage	Basic
CKM-03.2	The private and secret keys used for encryption shall be known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions	Substantial
CKM-03.3	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the cloud customer	Substantial
CKM-03.4	The private and secret keys used for encryption shall be known exclusively by the cloud customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements	High

CKM-04 SECURE KEY MANAGEMENT

Objective

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.

Requirements

Ref	Description	Ass. Level
CKM-04.1	Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; • Handling of compromised keys; and • Withdrawal and deletion of keys;	Basic
CKM-04.2	For the secure storage of keys, the key management system shall be separated from the application and middleware levels	Substantial
CKM-04.3	For the secure storage of keys and other secrets used for the administration tasks, the CSP shall use a suitable security container, software or hardware	High
CKM-04.4	If pre-shared keys are used, the specific provisions relating to the secure use of this procedure shall be specified separately.	Substantial

A.10 COMMUNICATION SECURITY

Ensure the protection of information in networks and the corresponding information processing systems

CS-01 TECHNICAL SAFEGUARDS

Objective

The CSP has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.

Requirements

Ref	Description	Ass. Level
CS-01.1	The CSP shall document, communicate and implement technical safeguards that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems, in accordance with ISP-02	Basic
CS-01.2	The technical safeguards in CS-01.1 shall be based on the results of a risk analysis carried out according to RM-01.	Substantial
CS-01.3	The CSP shall feed into a SIEM (Security Information and Event Management) system, all data from the technical safeguards implemented so that automatic countermeasures regarding correlating events are initiated	Substantial
CS-01.4	The CSP shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network	High
CS-01.5	The CSP shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines	High

Guidance elements	
CS-01.1	From C5. “on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial- of-Service (DDoS) attacks”

CS-02 SECURITY REQUIREMENTS TO CONNECT WITHIN THE CSP’S NETWORK

Objective

The establishment of connections within the CSP’s network is subject to specific security requirements.

Requirements

Ref	Description	Ass. Level
CS-02-1	The CSP shall document, communicate, make available and implement specific security requirements to connect within its network, including at least: • when the security zones are to be separated and when the cloud customers are to be logically or physically segregated; • what communication relationships and what network and application protocols are permitted in each case; • how the data traffic for administration and monitoring are segregated from each other at the network level; • what internal, cross-location communication is permitted; and • what cross-network communication is allowed.	Basic

CS-03 MONITORING OF CONNECTIONS WITHIN THE CSP'S NETWORK

Objective

The communication flows within the cloud, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.

Requirements

Ref	Description	Ass. Level
CS-03.1	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment	Basic
CS-03.2	The CSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable)	Basic
CS-03.2	The CSP shall design and configure both physical and virtualized network environments to restrict and monitor the connection to trusted or untrusted networks according to the defined security requirements (cf. CS-02)	Basic
CS-03.3	The CSP shall review at specified intervals the business justification for using all services, protocols, and ports. This review shall also include the compensatory measures used for protocols that are considered insecure	Basic
CS-03.4	The CSP shall review at least annually the design and implementation and configuration undertaken to monitor the connections in a risk-oriented manner, with regard to the defined security requirements	Substantial
CS-03.5	The CSP shall assess the risks of identified vulnerabilities in accordance with the risk management procedure (cf. RM-01) and follow-up measures shall be defined and tracked (cf.OPS-17)	Substantial
CS-03.6	The CSP shall protect all SIEM logs to avoid tampering	Substantial

CS-04 CROSS-NETWORK ACCESS

Objective

Cross-network access is restricted and only authorised based on specific security assessments.

Requirements

Ref	Description	Ass. Level
CS-04.1	Each network perimeter shall be controlled by security gateways	Basic
CS-04.2	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows	Substantial
CS-04.3	The system access authorisation for cross-network access shall be based on a security assessment based on the requirements of the cloud customers.	Substantial
CS-04.4	Each network perimeter shall be controlled by redundant and highly available security gateways	High
CS-04.5	The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1	High

CS-05 NETWORKS FOR ADMINISTRATION

Objective

Administrative and operational management duties are performed on networks segregated from other networks to prevent unauthorized traffics and to maintain separation of duties.

Requirements

Ref	Description	Ass. Level
CS-05.1	The CSP shall define and implement separate networks for the administrative management of the infrastructure and the operation of management consoles	Basic
CS-05.2	The CSP shall logically or physically separate the networks for administration from the CSCs' networks	Basic
CS-05.3	The CSP shall segregate physically or logically the networks used to migrate or create virtual machines	Basic
CS-05.4	When the administration networks are not physically segregated from other networks, the administration flows must be conveyed in a strongly encrypted tunnel.	High
CS-05.5	The CSP shall set up and configure an application firewall in order to protect the administration interfaces intended for CSCs and exposed over a public network	High

CS-06 TRAFFIC SEGREGATION IN SHARED NETWORK ENVIRONMENTS

Objective

The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.

Requirements

Ref	Description	Ass. Level
CS-06.1	The CSP shall define, document and implement segregation mechanisms at network level the data traffic of different cloud customers	Basic
CS-06.2	When implementing of infrastructure capabilities, the secure segregation shall be ensured by physically separated networks or by strongly encrypted VLANs	High

Guidance elements	
CS-06.2	The notion of strong encryption will be defined in the guidance for the CKM category

CS-07 NETWORK TOPOLOGY DOCUMENTATION

Objective

A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.

Requirements

Ref	Description	Ass. Level
CS-07.1	The CSP shall maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service	Basic
CS-07.2	The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with third-party and public networks, and the geographical locations in which the cloud customers' data are stored	Basic
CS-07.3	In liaison with the inventory of assets (cf. AM-01), the documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions.	Substantial
CS-07.4	The CSP shall perform a full review of the network topology documentation at least once a year	Substantial

CS-08 SOFTWARE DEFINED NETWORKING

Objective

Software-defined networking is only used if the cloud user data is protected by appropriate measures.

Requirements

Ref	Description	Ass. Level
CS-08.1	The CSP shall ensure the confidentiality of the cloud user data by suitable procedures when offering functions for software-defined networking (SDN)	Basic
CS-08.2	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features	Basic
CS-08.3	The CSP shall ensure that the configuration of networks matches network security policies regardless of the means used to create the configuration	Substantial

CS-09 DATA TRANSMISSION POLICIES

Objective

Policies are defined to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction.

Requirements

Ref	Description	Ass. Level
CS-09.1	The CSP shall document, communicate and implement policies and procedures with technical and organisational safeguards to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction, according to ISP-02	Basic
CS-09.2	The policy and procedures shall include references to the classification of assets (cf. AM-05)	Substantial

A.11 PORTABILITY AND INTEROPERABILITY

Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider

PI-01 DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES

Objective

Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems.

Requirements

Ref	Description	Ass. Level
PI-01.1	The cloud service shall be accessible by cloud services from other CSPs or cloud customers' IT systems through documented inbound and outbound interfaces	Basic
PI-01.2	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data	Basic
PI-01.3	Communication on these interfaces shall use standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements	Basic
PI-01.4	Communication over untrusted networks shall be encrypted according to CKM-02	Basic
PI-01.5	The CSP shall allow its customers to verify the interfaces provided (and their security) are adequate for its protection requirements before the start of the use of the cloud service, and each time the interfaces are changed	High

Guidance elements	
PI-01.1	From C5. "The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces"

PI-02 CONTRACTUAL AGREEMENTS FOR THE PROVISION OF DATA

Objective

Contractual agreements define adequate information with regard to the migration of data following the termination of the contractual relationship.

Requirements

Ref	Description	Ass. Level
PI-02.1	The CSP shall include in cloud service contractual agreements, at least, the following aspects concerning the termination of the contractual relationship: • Type, scope and format of the data the CSP provides to the CSC; • Delivery methods of the data to the cloud customer; • Definition of the timeframe, within which the CSP makes the data available to the CSC; • Definition of the point in time as of which the CSP makes the data inaccessible to the CSC and deletes these; and • The CSC's responsibilities and obligations to cooperate for the provision of the data.	Basic

Ref	Description	Ass. Level
PI-02.2	The definitions in PI-02.1 shall be based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the CSP as well as legal and regulatory requirements	Substantial
PI-02.3	The CSP shall identify, at least once a year, legal and regulatory requirements that may apply to these aspects and adjust the contractual agreements accordingly	High

PI-03 SECURE DELETION OF DATA

Objective

Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems.

Requirements

Ref	Description	Ass. Level
PI-03.1	The CSP shall implement procedures for deleting its customers' data upon termination of their contract in compliance with the contractual agreements between them	Basic
PI-03.2	The CSC's data deletion shall include metadata and data stored in the data backups as well	Basic
PI-03.3	The cloud customer's data deletion procedures shall prevent recovery by forensic means	Substantial
PI-03.4	The CSP shall document the deletion of the customer's data, including metadata and data stored in the data backups, in a way allowing the cloud customer to track the deletion of its data	Substantial
PI-03.5	At the end of the contract, the CSP shall delete the technical data concerning the client	Substantial

Guidance elements	
PI-03.5	From SecNumCloud. Such as "directory, certificates, access configuration"

A.12 CHANGE AND CONFIGURATION MANAGEMENT

Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service

CCM-01 POLICIES FOR CHANGES TO INFORMATION SYSTEMS

Objective

Policies and procedures are defined to control changes to information systems.

Requirements

Ref	Description	Ass. Level
CCM-01.1	The CSP shall document, implement, and communicate policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02	Basic
CCM-01.2	The change management policies and procedures shall cover at least the following aspects: • Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals; • Requirements for the performance and documentation of tests; • Requirements for segregation of duties during planning, testing, and release of changes; • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; • Requirements for the documentation of changes in the system, operational and user documentation; and • Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.	Substantial

CCM-02 RISK ASSESSMENT, CATEGORISATION AND PRIORITISATION OF CHANGES

Objective

Responsibilities are assigned inside the CSP organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Requirements

Ref	Description	Ass. Level
CCM-02.1	The CSP shall categorize and prioritize changes considering the potential security effects on the system components concerned	Basic
CCM-02.2	The CSP shall base the decision on classification and prioritization on a risk assessment performed in accordance with RM-01 with regard to potential effects on the system components concerned	Substantial
CCM-02.3	If the risk associated to a planned change is high, then appropriate mitigation measures shall be taken before deploying the service	High
CCM-02.4	In accordance with contractual agreements, the CSP shall submit to authorised bodies of the CSC meaningful information about the occasion, time, duration, type and scope of the change so that they can carry out their own risk assessment before the change is made available in the production environment	High
COM-02.5	Regardless of contractual agreements, the CSP shall inform the CSC as mentioned in CCM-02.3 for changes that have the highest risk category based on their risk assessment	High

CCM-03 TESTING CHANGES

Objective

Changes to the cloud services are tested before deployment to minimize the risks of failure upon implementation.

Requirements

Ref	Description	Ass. Level
CCM-03.1	The CSP shall test proposed changes before deployment	Basic
CCM-03.2	The type and scope of the tests shall correspond to the risk assessment	Substantial
CCM-03.3	The tests shall be carried out by appropriately qualified employees or by automated test procedures that comply with the state-of-the-art	Substantial
CCM-03.4	In accordance with contractual requirements, the CSP shall involve CSCs into the tests.	Substantial
CCM-03.5	The CSP shall first obtain approval from CSC and anonymise customer data before using it for tests, and shall guarantee the confidentiality of the data during the whole process	Substantial
CCM-03.6	The CSP shall determine the severity of the errors and vulnerabilities identified in the tests that are relevant for the deployment decision according to defined criteria, and shall initiate actions for timely remediation or mitigation	Substantial
CCM-03.7	The tests performed on a change before its deployment shall include tests on the service performed on a pre-production environment	High
CCM-03.8	The CSP shall document and implement a procedure that ensures the integrity of the test data used in pre-production	High
CCM-03.9	Before deploying changes on a system component, the CSP shall perform regression testing on other components of the cloud service that depend on that system component to verify the absence of undesirable effects	High
CCM-03.10	The CSP shall automatically monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues	High

Guidance elements	
CCM-03.3	The “state-of-the-art” will be defined in guidance

CCM-04 APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT

Objective

Changes to the cloud services are approved before being deployed in the production environment.

Requirements

Ref	Description	Ass. Level
CCM-04.1	The CSP shall approve any change to the cloud service, based on defined criteria, before they are made available to CSCs in the production environment	Basic
CCM-04.2	The CSP shall involve CSCs in the approval process according to contractual requirements	Substantial

Ref	Description	Ass. Level
CCM-04.3	The CSP shall automatically monitor the approvals of changes deployed in the production environment to guarantee fulfilment of CCM-04.1	High

Guidance elements	
CCM-04.1	The CSP's approval may be provided by authorised personnel of the CSP or by an automated procedure enforcing defined criteria.

CCM-05 PERFORMING AND LOGGING CHANGES

Objective

Changes to the cloud services are performed through authorized accounts and traceable to the person or system component who initiated them.

Requirements

Ref	Description	Ass. Level
CCM-05.1	The CSP shall define roles and rights according to IAM-01 for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment.	Basic
CCM-05.2	All changes to the cloud service in the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change	Basic
CCM-05.3	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1	High

CCM-06 VERSION CONTROL

Objective

Version control is used to track individual changes and enable restoration of a previous version if required.

Requirements

Ref	Description	Ass. Level
CCM-06.1	The CSP shall implement version control procedures to track the dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.	Basic
CCM-06.2	The version control procedures shall provide appropriate safeguards to ensure that the confidentiality, integrity and availability of cloud customer data is not compromised when system components are restored back to their previous state	High
CCM-06.3	The CSP shall retain a history of the software versions and of the systems that are implemented in order to be able to reconstitute, where applicable in a test environment, a complete environment such as was implemented on a given date; the retention time for this history shall be at least the same as that for backups (cf. OPS-06)	High

Guidance elements	
CCM-06.2	Availability can only be fully guaranteed for data that was present before the change, as data introduced by the change may be lost upon rollback.
CCM-06.3	Such a reconstitution of a test environment is intended to be used for investigations on the cloud service, and should not include the restoration of customer data

A.13 DEVELOPMENT OF INFORMATION SYSTEMS

Ensure information security in the development cycle of information systems

DEV-01 POLICIES FOR THE DEVELOPMENT AND PROCUREMENT OF INFORMATION SYSTEMS

Objective

Policies are defined to define technical and organisational measures for the development of the cloud service throughout its lifecycle.

Requirements

Ref	Description	Ass. Level
DEV-01.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 with technical and organisational measures for the secure development of the cloud service.	Basic
DEV-01.2	The policies and procedures for secure development shall consider information security from the earliest phases of design	Basic
DEV-01.3	The policies and procedures for secure development shall be based on recognised standards and methods with regard to the following aspects: • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); • Security in operation (reaction to identified faults and vulnerabilities); and • Secure coding standards and practices (avoiding the introduction of vulnerabilities in code).	Substantial
DEV-01.4	The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools	Substantial

Guidance elements	
DEV-01.3	These policies and procedures should focus on the Secure Software Development Life Cycle (SSDLC); they are expected to impact procedures beyond the present category, and in particular in the CCM and OPS categories

DEV-02 DEVELOPMENT SUPPLY CHAIN SECURITY

Objective

The supply chain of system components is considered in development security.

Requirements

Ref	Description	Ass. Level
DEV-02.1	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its cloud service	Basic
DEV-02.2	The CSP shall document and implement policies for the use of third-party and open source software	Substantial
DEV-02.3	The CSP makes its list of dependencies available to customers upon request	Substantial

Ref	Description	Ass. Level
DEV-02.4	In procurement for the development of the cloud service, the CSP shall perform a risk assessment in accordance to RM-01 for every product	High

Guidance elements	
DEV-02.1	For its software components, the list of dependencies is often called Software Board of Materials (SBoM). In the context of [EUCSA], Article 51(d) requires the identification and documentation of known dependencies. Dependencies should include all software modules, libraries or APIs used, as well as development tools.
DEV-02.2	The policy should cover the following aspects: • Restrictions on component age; • Restrictions on outdated and EOL/EOS components; • Restrictions on components with known vulnerabilities; • Restrictions on public repository usage; • Restrictions on acceptable licenses; • Component update requirements; • Deny list of prohibited components and versions; and • Acceptable community contribution guidelines. This list is inspired from the OWASP requirements on open source software [OWASP CA].
DEV-02.4	The use of certified products may considerably simplify the implementation of this requirement, because of the security guarantees that such a certification can bring.

DEV-02 SECURE DEVELOPMENT ENVIRONMENT

Objective

The development environment takes information security in consideration.

Requirements

Ref	Description	Ass. Level
DEV-03.1	The CSP shall ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development	Basic
DEV-03.2	The CSP shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers	Basic
DEV-03.3	The CSP shall implement a secure development and test environments that makes it possible to manage the entire development cycle of the information system of the cloud service	Substantial
DEV-03.4	The CSP shall consider the development and test environments when performing risk assessment	Substantial
DEV-03.5	The CSP shall include development resources as part of the backup policy	Substantial

Guidance elements	
DEV-03.5	Development resources include, among others, source code, databases, development and operation tools and their configurations.

DEV-04 SEPARATION OF ENVIRONMENTS

Objective

The development environment takes information security in consideration.

Requirements

Ref	Description	Ass. Level
DEV-04.1	The CSP shall ensure that production environments are physically or logically separated from development, test or pre-production environments	Basic
DEV-04.2	Data contained in the production environments shall not be used in development, test or pre-production environments in order not to compromise their confidentiality	Basic
DEV-04.3	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment	High

Guidance elements	
DEV-04.2	There is another requirement (CCM-03.5), in particular for pre-production environments that allows CSPs to derive test data from production data following specific requirements, but production data should never be used directly for testing purposes

DEV-05 DEVELOPMENT OF SECURITY FEATURES

Objective

The development environment takes information security in consideration.

Requirements

Ref	Description	Ass. Level
DEV-05.1	The CSP shall document, communicate, make available and implement specific procedures for the development of functions that implement technical mechanisms or safeguards required by the EUCS scheme, with increased testing requirements.	Basic
DEV-05.2	Design documentation for security features shall include a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature	Substantial
DEV-05.3	The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.	Substantial
DEV-05.4	The documentation of the tests for security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test.	Substantial
DEV-05.5	The documentation of the tests shall include a demonstration of the coverage of the source code, including branch coverage for security-critical code.	High

Guidance elements	
DEV-05.1	This requirement is applicable at all levels. For levels Substantial and High, it is refined by the following requirements. For level Basic, the following requirements from level Substantial should be considered as a suitable way to meet the requirement.

DEV-06 IDENTIFICATION OF VULNERABILITIES OF THE CLOUD SERVICE

Objective

Appropriate measures are taken to identify vulnerabilities introduced in the cloud service during the development process.

Requirements

Ref	Description	Ass. Level
DEV-06.1	The CSP shall apply appropriate measures to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process.	Basic
DEV-06.2	The procedures for identifying vulnerabilities shall be integrated in the development process.	Basic
DEV-06.3	The procedures shall include the following activities, depending on the risk assessment: • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.	Substantial
DEV-06.4	Code reviews shall be regularly performed by qualified personnel or contractors	High
DEV-06.5	The CSP shall assess the severity of identified vulnerabilities according to the criteria defined in OPS-17 and measures are taken to immediately eliminate or mitigate them.	Substantial
DEV-06.6	The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts, as part of the annual programme defined in OPS-19	High

Guidance elements	
DEV-06.1 DEV-06.2	For the Basic level, the measures are expected to be simple and automated, but some measures shall nonetheless be present to match the requirement from the EUCSA.
DEV-06.3	Because of the dependency on risk assessment, it is foreseen that many of the measures will be used at the High level.
DEV-06.3	The notion of code review is to be taken in a wide definition, not only limited to source code, but also applying to configuration files and more generally all content created by developers that may affect the security of the cloud service.

DEV-07 OUTSOURCING OF THE DEVELOPMENT

Objective

Outsourced developments provide similar security guarantees than in-house developments.

Requirements

Ref	Description	Ass. Level
DEV-07.1	When outsourcing development of the cloud service or components thereof to a contractor, the CSP and the contractor shall contractually agree on specifications regarding at least the following aspects: • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; • Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.	Basic
DEV-07.2	Before subcontracting the development of the cloud service or components thereof, the CSP shall conduct a risk assessment according to RM-01 that considers at least the following aspects • Management of source code by the subcontractor; • Human resource procedures implemented by the subcontractor; and • Required access to the CSP's development, testing and pre-production environments.	Substantial
DEV-07.3	The CSP shall document and implement a procedure that makes it possible to supervise and control the outsourced development activity, in order to ensure that the outsourced development activity is compliant with the secure development policy of the service provider and makes it possible to achieve a level of security of the external development that is equivalent to that of internal development	High
DEV-07.4	Internal or external employees of the CSP shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.	High

A.14 PROCUREMENT MANAGEMENT

Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements

PM-01 POLICIES AND PROCEDURES FOR CONTROLLING AND MONITORING THIRD PARTIES

Objective

Responsibilities are assigned inside the CSP organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Requirements

Ref	Description	Ass. Level
PM-01.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for controlling and monitoring third parties whose products or services contribute to the provision of the cloud service:	Basic
PM-01.2	The policies and procedures defined in PM-01.1 shall cover at least the following aspects: • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the CSP; • Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; • Information security awareness and training requirements for staff; • Applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents, and malfunctions; • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers, also contribute to the provision of the cloud service.	Substantial
PM-01.3	The CSP shall contractually require its subservice organizations to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system with respect to the EUCS requirements.	High
PM-01.4	The reports shall include the complementary subservice organisation controls that are required, together with the controls of the Cloud Service Provider, to meet the applicable EUCS requirements with reasonable assurance	High
PM-01.5	In case the supplier organizations are not able to provide an EUCS compliance report, the CSP shall reserve the right to audit them to assess the suitability and effectiveness of the service-related internal and complementary controls by qualified personnel	High

Guidance elements	
Terminology	Note that the term “supplier” covers both third parties that sell products and those who provide services.
PM-01.3	The requirement PM-01.5 is considered as an acceptable compensating requirement

PM-02 RISK ASSESSMENT OF SUPPLIERS

Objective

Suppliers of the CSP undergo a risk assessment to determine the security needs related to the product or service they provide.

Requirements

Ref	Description	Ass. Level
PM-02.1	The CSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties before they start contributing to the provision of the cloud service:	Basic
PM-02.2	The risk assessment shall include the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: • Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; • The CSP's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives.	Substantial
PM-02.3	Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of Complementary Subservice Organization Controls (CSOC) to be implemented by the subservice provider	Basic
PM-02.4	The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available evidence supporting the assessment of their effectiveness to the targeted evaluation level	Basic
PM-02.5	The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually	Basic

Guidance elements	
PM-02.4 PM-02.5	This is intended to prepare the work on dependencies. During the main audit, the auditor verifies the availability of assurance documentation, but the verification of that documentation is performed in a separate task.

PM-03 DIRECTORY OF SUPPLIERS

Objective

A centralized directory of suppliers is available to facilitate their control and monitoring.

Requirements

Ref	Description	Ass. Level
PM-03.1	The CSP shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the cloud service	Basic
PM-03.2	The directory shall contain the following information: • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the service provider/supplier; • Responsible contact person at the cloud service provider;	Substantial

Ref	Description	Ass. Level
	• Description of the service; • Classification based on the risk assessment; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements.	
PM-03.3	The CSP shall verify the directory for completeness, accuracy and validity at least annually	Basic

PM-04 MONITORING OF COMPLIANCE WITH REQUIREMENTS

Objective

Monitoring mechanisms are in place to ensure that third parties comply with their regulatory and contractual obligations.

Requirements

Ref	Description	Ass. Level
PM-04.1	The CSP shall monitor the compliance of its suppliers with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties	Basic
PM-04.2	Monitoring activities shall include at least a regular review of the following evidence, as provided by suppliers under contractual agreements: • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards; • independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents, and malfunctions.	Substantial
PM-04.3	The frequency of the monitoring shall correspond to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. PM-02), and the results of the monitoring shall be included in the review of the third party's risk assessment.	Basic
PM-04.4	Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf. RM-01)	Basic
PM-04.5	When a change in a third-party contributing to the delivery of the cloud service affects its level of security, the CSP shall inform all of its CSCs without delay	Basic
PM-04.6	The CSP shall document and implement a procedure to review and update, at least once a year, non-disclosure or confidentiality requirements regarding suppliers contributing to the delivery of the service	Substantial
PM-04.7	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling).	High
PM-04.8	The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action	High

Guidance elements	
PM-04.7 PM-04.8	This automated monitoring may also lead to the identification of nonconformities, which may need to be reported to the CAB as part of the CSP's continuous monitoring obligations.

PM-05 EXIT STRATEGY

Objective

Strategies are documented that ensure minimum business disruption if the relationship with a supplier is terminated.

Requirements

Ref	Description	Ass. Level
PM-05.1	The CSP shall define exit strategies for the purchase of services where the risk assessment of the suppliers identified a very high dependency	Basic
PM-05.2	The exit strategies shall be aligned with operational continuity plans and include the following aspects: • Analysis of the potential costs, impacts, resources, and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities, and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; • Definition of indicators for service performance monitoring, which should initiate the withdrawal from the service if the results are unacceptable.	Substantial

A.15 INCIDENT MANAGEMENT

Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents

IM-01 POLICY FOR SECURITY INCIDENT MANAGEMENT

Objective

A policy is defined to respond to security incidents in a fast, efficient and orderly manner.

Requirements

Ref	Description	Ass. Level
IM-01.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 containing technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents:	Basic
IM-01.2	The policies and procedures shall include guidelines for the classification, prioritization, and escalation of security incidents and creates interfaces for incident management and business continuity management	Basic
IM-01.3	The CSP shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents	Basic
IM-01.4	The CSP shall inform the customers affected by security incidents in a timely and appropriate manner	Substantial
IM-01.5	The incident management policy shall include procedures as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident	Substantial
IM-01.6	The incident management policy shall include analysis plans for typical security incidents	High
IM-01.7	The incident management policy shall include an evaluation methodology so that the collected information does not lose its evidential value in any subsequent legal assessment	High
IM-01.8	The incident management policy shall include provisions for the regular testing of the incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential deficiencies	High

Guidance elements	
IM-01.3	At level Basic, the CERT may be a simplified organization that supervises the response to incidents

IM-02 PROCESSING OF SECURITY INCIDENTS

Objective

A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.

Requirements

Ref	Description	Ass. Level
IM-02.1	The CSP shall classify, prioritize, and perform root-cause analyses for events that could constitute a security incident, using their subject matter experts and external security providers where appropriate	Basic
IM-02.2	The CSP shall maintain a catalogue that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents	Substantial
IM-02.3	The incident classification mechanism shall include provisions to correlate events. In addition, these correlated events shall themselves be assessed and classified according to their criticality	Substantial
IM-02.4	The CSP shall simulate the identification, analysis, and defence of security incidents and attacks at least once a year through appropriate tests and exercises	High
IM-02.5	The CSP shall monitor the processing of incident to verify the application of incident management policies and procedures	High

Guidance elements	
IM-02.4	From C5 “e.g., Red Team training”
IM-02.5	Typical monitoring could occur through analysis a ticket management or other business process management system

IM-03 DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS

Objective

Security incidents are documented to and reported in a timely manner to customers.

Requirements

Ref	Description	Ass. Level
IM-03.1	The CSP shall document the implemented measures after a security incident has been processed and, following the contractual agreements, the document shall be sent to the affected customers for final acknowledgment or, if applicable, as confirmation.	Basic
IM-03.2	The CSP shall make information on security incidents or confirmed security breaches available to all affected customers	Basic
IM-03.3	The CSP shall continuously report on security incidents to affected customers until the security incident is closed and a solution is applied and documented, in accordance to the defined SLA and contractual agreements	Substantial
IM-03.4	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period	High

IM-04 USER’S DUTY TO REPORT SECURITY INCIDENTS

Objective

Security incidents are documented to and reported in a timely manner to customers.

Requirements

Ref	Description	Ass. Level
IM-04.1	The CSP shall inform employees and external business partners of their contractual obligations to report all security events that become known to them and are directly related to the cloud service	Basic
IM-04.2	The CSP shall not take any negative action against those who communicate "false reports" of events that do not subsequently turn out to be incidents, and shall make that policy known as part of its communication to employees and external business partners	Basic
IM-04.3	The CSP shall define, make public and implement a single point of contact to report security events and vulnerabilities	Basic

IM-05 INVOLVEMENT OF CLOUD CUSTOMERS IN THE EVENT OF INCIDENTS

Objective

Customers are kept regularly informed of the status incidents that concern them.

Requirements

Ref	Description	Ass. Level
IM-05.1	The CSP shall periodically inform its customers on the status of the incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual agreements	Basic
IM-05.2	As soon as an incident has been closed, The CSP shall inform its customers about the actions taken, according to the contractual agreements	Basic

IM-06 EVALUATION AND LEARNING PROCESS

Objective

Measures are in place to continuously improve the service from experience learned in incidents.

Requirements

Ref	Description	Ass. Level
IM-06.1	The CSP shall perform an analysis of security incidents to identify recurrent or significant incidents and to identify the need for further protection, if needed with the support of external bodies	Basic
IM-06.2	The CSP shall only contract supporting external bodies that are qualified incident response service providers or government agencies	Basic
IM-06.3	The CSP shall define, implement and maintain a knowledge repository of security incidents and the measures taken to solve them, as well as information related to the assets that these incidents affected, and use that information to enrich the classification catalogue	Substantial
IM-06.4	The intelligence gained from the incident management and gathered in the knowledge repository shall be used to identify recurring incidents or potential significant incidents and to determine the need for advanced safeguards and implement them	Substantial

IM-07 INCIDENT EVIDENCE PRESERVATION

Objective

Measures are in place to preserve information related to security incidents.

Requirements

Ref	Description	Ass. Level
IM-07.1	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents	Basic
IM-07.2	The documents and evidence shall be archived in a way that could be used as evidence in court	Substantial
IM-07.3	When the CSP requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the CSP shall contract a qualified incident response service provider only	Substantial
IM-07.4	The CSP shall implement security mechanisms and processes for protecting all the information related to security incidents in accordance with criticality levels and legal requirements in effect	Basic
IM-07.5	The service provider shall establish an integrated team of forensic/incident responder personnel specifically trained on evidence preservation and chain of custody management	High

A.16 BUSINESS CONTINUITY

Plan, implement, maintain and test procedures and measures for business continuity and emergency management

BC-01 BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY

Objective

Responsibilities are assigned inside the CSP organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.

Requirements

Ref	Description	Ass. Level
BC-01.1	The CSP shall document, communicate and make available policies and procedures establishing the strategy and guidelines to ensure business continuity and contingency management	Basic
BC-01.2	The CSP shall name (a member of) top management as the process owner of business continuity and emergency management, and responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines, and for ensuring that sufficient resources are made available for an effective process	Substantial
BC-01.3	The business continuity and contingency management process owner shall ensure that sufficient resources are made available for an effective process	Substantial

BC-02 BUSINESS IMPACT ANALYSIS PROCEDURES

Objective

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the cloud service or enterprise.

Requirements

Ref	Description	Ass. Level
BC-02.1	The policies and procedures for business continuity and contingency management shall include the need to perform a business impact analysis to determine the impact of any malfunction to the cloud service or enterprise.	Basic
BC-02.2	The business impact analysis policies and procedures shall consider at least the following aspects: • Possible scenarios based on a risk analysis; • Identification of critical products and services; • Identification of dependencies, including processes (including resources required), applications, business partners and third parties; • Identification of threats to critical products and services; • Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and • Estimation of the resources needed for resumption.	Substantial
BC-02.3	The business impact analysis resulting from these policies and procedures shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Substantial

BC-03 BUSINESS CONTINUITY AND CONTINGENCY PLANNING

Objective

A business continuity framework including a business continuity plan and associated contingency plans is available.

Requirements

Ref	Description	Ass. Level
BC-03.1	The CSP shall document and implement a business continuity plan and contingency plans to ensure continuity of the services, taking into account information security constraints and the results of the business impact analysis	Basic
BC-03.2	The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used	Substantial
BC-03.3	The business continuity plan and contingency plans shall cover at least the following aspects: • Defined purpose and scope, including relevant business processes and dependencies; • Accessibility and comprehensibility of the plans for persons who are to act accordingly; • Ownership by at least one designated person responsible for review, updating and approval; • Defined communication channels, roles and responsibilities including notification of the customer; • Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers); • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management.	Substantial
BC-03.4	The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Substantial

BC-04 BUSINESS CONTINUITY TESTS AND EXERCISES

Objective

The business continuity framework is tested on a regular basis.

Requirements

Ref	Description	Ass. Level
BC-04.1	The business impact analysis, business continuity plan and contingency plans shall be tested at regular intervals (at least once a year) or after an update	Substantial
BC-04.2	The tests shall be documented and the results considered to update the business continuity plan and to define future operational continuity measures	Substantial
BC-04.3	The tests shall involve CSCs and relevant third parties, such as external service providers and suppliers	Substantial
BC-04.4	In addition to the tests, exercises shall also be carried out, which are, among other things, based on scenarios resulting from security incidents that have already occurred in the past	High

A.17 COMPLIANCE

Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements

CO-01 IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS

Objective

The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service are defined and documented.

Requirements

Ref	Description	Ass. Level
CO-01.1	The CSP shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service	Basic
CO-01.2	The CSP shall document and implement procedures for complying to these contractual requirements	Substantial
CO-01.3	The CSP shall provide these procedures when requested by a CSC	High
CO-01.4	The CSP shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the service	High

Guidance elements	
CO-01.1	Typically, such requirements may include: • Requirements for the protection of personal data (e.g. EU General Data Protection Regulation); • Compliance requirements based on contractual obligations with cloud customers (e.g. ISO/IEC 27001, SOC 2, PCI-DSS); • Generally accepted accounting principles (e.g. in accordance with HGB or IFRS); • National laws

CO-02 POLICY FOR PLANNING AND CONDUCTING AUDITS

Objective

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the cloud service.

Requirements

Ref	Description	Ass. Level
CO-02.1	The CSP shall document, communicate, make available and implement policies and procedures for planning and conducting audits, made in accordance with ISP-02 and addressing at least the following aspects: • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities.	Basic

Ref	Description	Ass. Level
CO-02.2	The CSP shall document and implement an audit programme over three years that defines the scope and the frequency of the audits in accordance with the management of change, policies, and the results of the risk assessment	Substantial
CO-02.3	The CSP shall grant its CSCs contractually guaranteed information and define their audit rights	High

Guidance elements	
CO-02.2	The audit programme should provide a high-level description of the audits to be provided in the following three years

CO-03 INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM

Objective

Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.

Requirements

Ref	Description	Ass. Level
CO-03.1	The CSP shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control system to the requirements defined in CO-01.	Basic
CO-03.2	The internal audit shall check the compliance with the requirements of the scheme at the targeted EUCS assurance level.	Basic
CO-03.3	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure (cf. RM-01) and follow-up measures are defined and tracked (cf. OPS-17).	Substantial
CO-03.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions	High
CO-03.5	The CSP shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate CSP's subject matter experts for immediate assessment and action	High
CO-03.6	The CSP shall document specifically deviations that are nonconformities from the EUCS requirements, including an assessment of their severity, and keep track of their remediation	Basic
CO-03.7	The CSP shall inform CSCs who operate an EUCS-certified cloud service of nonconformities relatively to EUCS requirements	Substantial

Guidance elements	
CO-03.6	In particular, the scheme requires that the CSP notify its CAB of major nonconformities
CO-03.7	This is a requirement for composition, to ensure that nonconformities are properly transmitted across the supply chain

CO-04 INFORMATION ON INTERNAL CONTROL SYSTEM ASSESSMENT

Objective

The top management of the CSP is kept informed of the performance of the internal control system in order to ensure its continued suitability, adequacy and effectiveness

Requirements

Ref	Description	Ass. Level
CO-04.1	The CSP shall regular inform its top management about the information security performance within the scope of the internal control system.	Basic
CO-04.2	This information shall be included in the management review of the internal control system that is performed at least once a year	Substantial

A.18 USER DOCUMENTATION

Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers

DOC-01 GUIDELINES AND RECOMMENDATIONS FOR CLOUD CUSTOMERS

Objective

Provide information to assist the cloud customer in the secure configuration, installation and use of the cloud service.

Requirements

Ref	Description	Ass. Level
DOC-01.1	The CSP shall make publicly available guidelines and recommendations to assist CSCs with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided	Basic
DOC-01.2	The guidelines and recommendations for the secure use of the cloud service shall cover at least the following aspects, where applicable to the cloud service: • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms; • Roles and rights concept including combinations that result in an elevated risk; • Services and functions for administration of the cloud service by privileged users, and • Complementary Customer Controls (CCCs).	Substantial
DOC-01.3	The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use	Basic
DOC-01.4	The CSP shall describe in the user documentation all risks shared with the customer	Substantial
DOC-01.5	The CSP shall regularly analyse how the CSCs apply the security recommendations and CCCs, and take measure to encourage compliance based on the defined shared responsibility model	High

Guidance elements	
DOC--01.4	This requirement is related to the acceptance of risk by risk owners in the risk management procedures (cf. RM-03). Add reference to CCCs

DOC-02 ONLINE REGISTER OF KNOWN VULNERABILITIES

Objective

Provide information to assist the cloud customer in the secure configuration, installation and use of the cloud service.

Requirements

Ref	Description	Ass. Level
DOC-02.1	The CSP shall operate or refer to a publicly available and daily updated online register of known vulnerabilities that affect the provided cloud service	Basic

Ref	Description	Ass. Level
DOC-02.2	The online register of vulnerabilities shall also include known vulnerabilities that affect assets provided by the CSP that the cloud customers have to install, provide or operate themselves under the customers responsibility	Substantial
DOC-02.3	The presentation of the vulnerabilities shall follow an industry-accepted scoring system for the description of vulnerabilities	Substantial
DOC-02.4	The information contained in the online register shall include sufficient information to form a suitable basis for risk assessment and possible follow-up measures on the part of cloud users	Substantial
DOC-02.5	For each vulnerability, the online register shall indicate whether software updates are available, when they will be rolled out and whether they will be deployed by the CSP, the CSC or both	Substantial
DOC-02.6	The CSP shall equip with automatic update mechanisms the assets it provides that must be installed, provided or operated by CSCs within their area of responsibility	High

Guidance elements	
DOC--02.3	The Common Vulnerability Scoring System (CVSS) should be used.

DOC-03 LOCATIONS OF DATA PROCESSING AND STORAGE

Objective

Provide transparent information about the location of the data and of its processing.

Requirements

Ref	Description	Ass. Level
DOC-03.1	The CSP shall provide comprehensible and transparent information on: • Its jurisdiction; and • System component locations, including its subcontractors, where the cloud customer's data is processed, stored and backed up.	Basic
DOC-03.2	The CSP shall provide sufficient information for subject matter experts of the CSC to determine to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective	Basic
DOC-03.3	The CSP shall provide information about • The locations from administration and supervision may be carried out on the cloud service; • The locations to which any cloud customer data, meta-data or derived data may be transferred, processed or stored.	Substantial
DOC-03.4	The CSP shall document the locations from which it conducts support operations for clients, and it shall document the list of operations that can be carried by client support in each location	High

Guidance elements	
DOC--03.2	In particular, if the CSP uses subservice providers that are certified in the EUCS scheme, the CSP shall include the all relevant from that subservice provider in their own description.

DOC-04 JUSTIFICATION OF THE TARGETED ASSURANCE LEVEL

Objective

Provide a rationale for the assurance level target by the cloud service.

Requirements

Ref	Description	Ass. Level
DOC-04.1	The CSP shall provide a justification for the assurance level targeted in the certification, based on the risks associated to the cloud service's targeted users and use cases	Basic
DOC-04.2	If the CSP claims compliance to security profiles for its cloud service, the justification shall cover the security profiles.	Basic
DOC-04.3	A summary of the justification shall be made publicly available as part of the certification package, which shall allow CSCs to perform a high-level analysis about their own use cases	Basic
DOC-04.4	The justification shall be based on a risk analysis according to RM-01	Substantial

DOC-05 GUIDELINES AND RECOMMENDATIONS FOR COMPOSITION

Objective

Provide the information required by customers that want to use the cloud service as a base service for their own certified cloud service.

Requirements

Ref	Description	Ass. Level
DOC-05.1	If the CSP expects CSCs to certify with EUCS their own services based on its cloud service using composition, it shall provide specific documentation for them, based on the Complementary Customer Controls (CCCs) that they have defined	Basic
DOC-05.2	The CSP shall include in the description provided for each CCC a list of actionable requirements for the CSC, and it shall associate each CCC to an EUCS requirement	Basic
DOC-05.3	The CSP shall make the documentation defined in DOC-05.1 available to cloud customers upon request	Basic
DOC-05.4	The CSP shall label each requirement associated to a CCC with the lowest EUCS assurance level for which it is required	Substantial

Guidance elements	
DOC--05.1	The expectation of the CSP needs to be declared in the application document, as the CAB should be aware that this documentation should be available, and should also be included in the audit.

DOC-06 CONTRIBUTION TO THE FULFILMENT OF REQUIREMENTS FOR COMPOSITION

Objective

Provide the information required by customers that want to use the CSP as subservice organization for the cloud service

Requirements

Ref	Description	Ass. Level
DOC-06.1	If the CSP expects CSCs to certify with EUCS their own services based on its cloud service using composition, it shall document for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of the requirement by the cloud service developed by the CSC using the CSP as subservice organization.	Basic
DOC-06.2	The CSP shall make the documentation defined in DOC-06.1 available to cloud customers upon request	Basic
DOC-06.3	The CSP shall justify the contributions in a companion document	Substantial

A.19 DEALING WITH INVESTIGATION REQUESTS FROM GOVERNMENT AGENCIES

Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data

INQ-01 LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRIES

Objective

Investigative inquiries are assessed before determining further steps to be taken.

Requirements

Ref	Description	Ass. Level
INQ-01.1	The CSP shall subject investigation requests from government agencies to a legal assessment by subject matter experts	Basic
INQ-01.2	The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken	Basic

INQ-02 INFORMING CLOUD CUSTOMERS ABOUT INVESTIGATION REQUESTS

Objective

Cloud customers are kept informed of ongoing investigations if legally permitted.

Requirements

Ref	Description	Ass. Level
INQ-02.1	The CSP shall inform the affected CSC(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service	Basic

INQ-03 CONDITIONS FOR ACCESS TO OR DISCLOSURE OF DATA IN INVESTIGATION REQUESTS

Objective

Investigators only have access to the data required for their investigation after validation of the legality of their request.

Requirements

Ref	Description	Ass. Level
INQ-03.1	The CSP shall only provide access to or disclose cloud customer data in the context of government investigation requests after the CSP's legal assessment (cf. INQ-01) has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis.	Basic
INQ-03.2	The CSP shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate	Basic

Ref	Description	Ass. Level
INQ-03.3	When no clear limitation of the data is possible, the CSP shall anonymise or pseudonymise the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request	Substantial
INQ-03.4	The CSP shall automatically monitor the accesses performed by or on behalf of investigators to ensure that they correspond to the determined legal basis	High

A.20 PRODUCT SAFETY AND SECURITY (PSS)

Provide appropriate mechanisms for cloud customers

Foreword for Reviewers

There is an ongoing discussion on the PSS category, as some of the PSS sections have been moved to other categories:

- PSS-01 and PSS-03 have been moved to DOC;
- PSS-02 has been moved to DEV;
- PSS-05, PSS-07, PSS-08 and PSS-09 have been integrated into IAM; and
- PSS-11 has been moved to CO.

For the objectives and requirements listed below, the question remains open. The original C5 numbers have been kept for clarity

PSS-01 ERROR HANDLING AND LOGGING MECHANISMS

Objective

Cloud customers have access to sufficient information about the cloud service through error handling and logging mechanisms.

Requirements

Ref	Description	Ass. Level
PSS-01.1	The CSP shall offer to their CSCs error handling and logging mechanisms that allow them to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides	Basic
PSS-01.2	The information provided shall be detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: • Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); • Malfunctions during processing of automatic or manual actions; and • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security.	Substantial
PSS-01.3	The logged information shall be protected from unauthorised access and modification and can be deleted by the CSC	Substantial
PSS-01.4	When the CSC is responsible for the activation or type and scope of logging, the CSP shall provide appropriate logging capabilities	Substantial
PSS-01.5	The CSP shall make the information available to CSCs via documented interfaces that are suitable for further processing this information as part of their Security Information and Event Management (SIEM).	High

PSS-02 SESSION MANAGEMENT

Objective

A suitable session management is used to protect confidentiality, availability, integrity and authenticity during interactions with the cloud service.

Requirements

Ref	Description	Ass. Level
PSS-02.1	A suitable session management system shall be used that at least corresponds to the state-of-the-art and is protected against known attacks	Basic
PSS-02.2	The session management system shall include mechanisms that invalidate a session after it has been detected as inactive.	Substantial
PSS-02.3	If inactivity is detected by time measurement, the time interval shall be configurable by the CSP or – if technically possible – by the CSC	Substantial

Guidance elements	
PSS-02.1	The guidance will clarify the notion of “state-of-the-art”
PSS-02.3	The CSP should define an acceptable range and a default value for the time interval, and the CSC should have the ability to select a value within the acceptable range. In case of technical impossibility, it should be clearly demonstrated

PSS-03 SOFTWARE DEFINED NETWORKING

Objective

Software-defined networking is only used if the cloud user data is protected by appropriate measures.

Requirements

Ref	Description	Ass. Level
PSS-03.1	The CSP shall ensure the confidentiality of the cloud user data by suitable procedures when offering functions for software-defined networking (SDN)	Basic
PSS-03.2	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features	Basic
PSS-03.3	The CSP shall ensure that the configuration of networks matches network security policies regardless of the means used to create the configuration	Substantial

PSS-04 IMAGES FOR VIRTUAL MACHINES AND CONTAINERS

Objective

Services for providing and managing virtual machines and containers to customers include appropriate protection measures.

Requirements

Ref	Description	Ass. Level
PSS-04.1	The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: • The CSC can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this CSC can only launch the images or containers released according to these restrictions. • In addition, these images provided by the CSP are hardened according to generally accepted industry standards.	Basic
PSS-04.2	The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: • If the CSP provides images of virtual machines or containers to the CSC, the CSP appropriately inform the CSC of the changes made to the previous version.	Substantial
PSS-04.3	An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images	High

PSS-05 LOCATIONS OF DATA PROCESSING AND STORAGE

Objective

Provide users with choices about the location of the data and of its processing.

Requirements

Ref	Description	Ass. Level
PSS-05.1	The CSP shall allow the CSC to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options	Substantial
PSS-05.2	All CSP commitments regarding locations of data processing and storage shall be enforced by the cloud service architecture	Substantial

Guidance elements	
PSS-05.2	The commitments referred to here also include those associated with the information disclosed in DOC-03