Ref	Description	Ass. Level	Applicable	Comment
AM-01.1	The CSP shall document and implement policies and procedures for maintaining an inventory of assets	Basic	no	No Maintainance of Asset Inventory
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	no	
AM-01.3	The CSP shall record for each asset the information needed to apply the risk management procedure defined in RM-01.	Basic	no	Protection need is defined, damage potential is unclear
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	partly	can be done for the already defined assets
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	no	not applicable without operation of the service
AM-01.6	The CSP shall automatically monitor the inventory of assets to guarantee it is up-to-date	High	no	not applicable without operation of the service
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	no	depends on the operator of the service
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	no	
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	no	

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	no	no comissioning of hardware
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	no	no comissioning of hardware
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	no	no comissioning of hardware
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	no	no comissioning of hardware
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	no	no comissioning of hardware
AM-03.6	The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.	High	no	no comissioning of hardware
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
AM-04.4	The verification of the commitment defined in AM-04.1 shall be automatically monitored	High	no	not applicable without operation of the service
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	partly	can be done for the already defined assets
AM-05.2	The asset classification schema shall provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives	Substantial	partly	can be done for the already defined assets
AM-05.3	When applicable, the CSP shall label all assets according to their classification in the asset classification schema	Basic	no	not applicable without operation of the service
AM-05.4	The need for protection shall be determined by the individuals or groups responsible for the assets	Substantial	no	not applicable without operation of the service

Ref	Description	Ass. Level	Applicable	Comment
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
OPS-01.3	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning	High	no	not applicable without operation of the service
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	no	out of scope of the development
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	no	not applicable without operation of the service
OPS-02.3	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1	High	no	out of scope of the development
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	no	out of scope of the development

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	no	out of scope of the development for this controll in depth systems specific knowledge is needed
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	no	out of scope of the development
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 customers self-service and the CSPs administration)	High	no	out of scope of the development
OPS-04.4	The CSP shall update the anti-malware products at the highest frequency that the vendors actually offer	High	no	out of scope of the development
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 procedure	Basic	no	out of scope of the development
OPS-05.2	Signature-based and behaviour-based malware protection tools shall be updated at least daily	Substantial	no	out of scope of the development
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	no	not applicable without operation of the service
OPS-05.4	The CSP shall automatically monitor the antimalware scans to track detected malware or irregularities	High	no	not applicable without operation of the service

OPS-06.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery	Basic	partly	proposal with important information regarding possible data to back-up can be provided
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	out of scope of the development
OPS-07.3	The CSP shall automatically monitor their data backups to guarantee fulfilment of OPS-07.1	High	no	not applicable without operation of the service
OPS-08.1	The CSP shall test the restore procedures at least annually	Basic	no	not applicable without operation of the service
OPS-08.2	The restore tests shall assess if the specifications for the RTO and RPO agreed with the customers are met	Substantial	no	not applicable without operation of the service
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	no	not applicable without operation of the service

OPS-08.4	The CSP shall inform CSCs, at their request, of the results of the recovery tests	High	no	not applicable without operation of the service
OPS-08.5	Recovery tests shall be included in the CSP’s business continuity management	High	no	not applicable without operation of the service
OPS-09.1	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
OPS-09.4	The physical and environmental security measures at the remote site shall have the same level as at the main site	Substantial	no	out of scope of the development
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	no	out of scope of the development
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	partly	See Logging documentation for components developed in this project

OPS-10.2	The policies and procedures shall cover at least the following aspects: * 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	Substantial	partly	Only the first point can be adressed by our project, see Logging documentation
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

OPS-11.4	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service
OPS-12.2	Identified events shall be reported to the appropriate departments for timely assessment and remediation.	Basic	no	not applicable without operation of the service
OPS-12.3	The monitoring of events mentioned in OPS-12.1 shall be automated	Substantial	no	out of scope of the development
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	no	not applicable without operation of the service
OPS-13.1	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation	Basic	no	out of scope of the development
OPS-13.2	Log data shall be deleted when it is no longer required for the purpose for which they were collected	Basic	no	out of scope of the development
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	no	out of scope of the development
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	no	out of scope of the development
OPS-13.5	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	no	out of scope of the development

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	no	not applicable without operation of the service
OPS-13.7	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service
OPS-14.2	The CSP shall make available interfaces to conduct forensic analysis and perform backups of infrastructure components and their network communication	Substantial	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	out of scope of the development
OPS-15.2	Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01)	Basic	no	not applicable without operation of the service
OPS-15.3	The access to system components for logging and monitoring shall require strong authentication	Substantial	no	out of scope of the development
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	partly	Logging in the developed components can be prepared
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	yes	Logging in the developed components can be prepared

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	partly	can be difened for the development in the project context
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	partly	the assesment part can be done for the vulnerabilities identified in the development, no other steps of this controll are otherwise applicaple without operating the service
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	yes	
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	partly	Can be prepared by writing a section about Infrastructure Security Scanning for the Security Concept
OPS-19.2	The CSP shall perform the tests defined in OPS-18.1 at least once a month	Substantial	no	In the EUCS these are both 19.2 not applicable without operation of the service
OPS-19.3	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	partly	In the EUCS these are both 19.2 A PenTest will be part of the Security Testing in the test phase. However a PenTest will provide the most useful insights if it is run in the final production env
OPS-19.4	The CSP shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures (cf. OPS-18).	Substantial	partly	PenTest will be performed in the course of the Security Testing
OPS-19.5	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	no	not applicable without operation of the service
OPS-19.6	Some of the penetration tests performed each year shall be performed by external service providers	High	no	not applicable without operation of the service
OPS-19.7	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	partly	PenTest results will be analysed

OPS-19.8	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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	High	no	not applicable without operation of the service
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	no	In the EUCS OPS-22.1 and OPS-21.1 are bothlabled as OPS-21.1 If we do not give out any component containing an OS this control is not applicable to us
OPS-21.2	The hardening requirements for each system component shall be documented	Basic	no	CIS Hardening Standards
OPS-21.3	The CSP shall automatically monitor the service components under its responsibility for compliance with hardening specifications	High	no	Checkov is used to scan the system for the recomended security configurations by the CIS Hardening standards

OPS-22.1	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	no	In the EUCS OPS-22.1 and OPS-21.1 are bothlabled as OPS-21.1 not applicable without operation of the service

Ref	Description	Ass. Level	Applicable	Comment
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IAM-01.3	The CSP shall base its access control policy on the use of role-based access control.	Substantial	no	not applicable without operation of the service
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	yes	

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 * 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	Substantial	no	not applicable without operation of the service
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	partly	
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	partly	
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	partly	

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	partly	
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	yes	
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	yes	
IAM-03.1	The CSP shall define and implement an automated mechanism to block user accounts after a certain period of time	Basic	unsure	
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	unsure	
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	unsure	
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	unsure	
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

IAM-03.7	The CSP shall implement the process in IAM-03.5 on all user accounts under its responsibility	High	no	not applicable without operation of the service
IAM-03.8	Approval from authorised personnel or system components is required to unlock accounts locked automatically	Substantial	unsure	
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	unsure	
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	unsure	
IAM-03.11	The CSP shall automatically monitor the implemented automated mechanisms to guarantee their compliance with IAM-03	High	unsure	
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	partly	Logging is done for failed login attempts, notification of the suers can not be done by us
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	yes	
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	unsure	
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	unsure	
IAM-04.6	The access right management procedures shall follow a dynamic approach	High	yes	
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	no	no privleged access rights for users
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	no privleged access rights for users
IAM-05.5	The CSP shall perform the review defined in IAM-05.1 at least every six (6) months	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	no privleged access rights for users
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	no	out of scope of the development
IAM-06.4	Shared accounts under the responsibility of the CSP shall be assigned only to internal or external employees	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IAM-06.7	The CSP shall require strong authentication for accessing the administration interfaces used by the CSP	Substantial	no	not applicable without operation of the service
IAM-06.8	The CSP shall require strong authentication for accessing the administration interfaces offered to the CSC	High	no	not applicable without operation of the service

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	partly	Document the authentication mechanism and document that there is only one kind of user account possible in the system
IAM-07.2	The access to all environments of the CSP shall be authenticated, including non-production environments	Substantial	no	not applicable without operation of the service
IAM-07.3	The access to the production environment of the CSP shall require strong authentication	High	no	not applicable without operation of the service
IAM-07.4	The access to all environments of the CSP containing CSC data shall require strong authentication	High	no	not applicable without operation of the service
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	yes	Using VCDM
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	no	not applicable without operation of the service
IAM-07.7	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts	Basic	unsure	
IAM-07.8	The CSP shall offer strong authentication methods to the CSC for use with the accounts under their responsibility	Substantial	yes	2FA by using QA-Code and VCDM

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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IAM-08.4	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01)	Basic	no	No passwords
IAM-08.5	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	Basic	yes	
IAM-08.6	When creating credentials, compliance with specifications is enforced automatically as far as technically possible	Substantial	no	no credential creation
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	unsure	
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	no	no passwords
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	no	not applicable without operation of the service

IAM-09.1	The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems	Basic	no	
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	no	
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	no	
IAM-09.4	The CSP shall implement suitable measures for partitioning between the CSCs	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
IAM-09.7	If the CSP offers to its CSCs interfaces for administrators and for end users, these interfaces shall be separated	Substantial	no	

Ref	Description	Ass. Level	Applicable	Comment
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	yes	Document all crypto algos
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	yes	We always choose the strongest possible encryption
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	yes	BSI technical recommondation
CKM-02.1	The CSP shall define and implement strong encryption mechanisms for the transmission of cloud customer data over public networks	Basic	yes	TLS
CKM-02.2	The CSP shall define, and implement strong encryption mechanisms for the transmission of all data over public networks	High	yes	TLS
CKM-03.1	The CSP shall document and implement procedures and technical safeguards to encrypt cloud customers' data during storage	Basic	partly	Use encrypted filesystem for storage of KexCloak database

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	yes	Using a KeyContainer to secure the crypto keys used for generation of access tokens (k8s secret)
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	no	not applicable without operation of the service
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	yes	Using a KeyContainer to secure the crypto keys used for generation of access tokens (k8s secret)
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	partly	can be partly prepared for, documentation about key management has to be present in the security concept currently only use one key, it's generated with system start up and secured by k8s secret
CKM-04.2	For the secure storage of keys, the key management system shall be separated from the application and middleware levels	Substantial	yes	k8s secret
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	yes	k8s secret

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	yes	IAT long term key and 2 secrets for clients use k8s secret storage for provisioning of the AAS service For KeyCloak this will have to be done manually --> document procedure

Ref	Description	Ass. Level	Applicable	Comment
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	partly	Logging Information can be collected and the system prepared to be able to ship logs to such systems
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	no	No risk analysis
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	partly	Logging Information can be collected and the system prepared to be able to ship logs to such systems
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	no	not applicable without operation of the service
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	no	Question regarding network segementation/security
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	partly	Documentation has to show how to connect the IAM Platform (if an already existing IAM platform is used)

CS-03.1	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment	Basic	partly	This is partly considered in the architecture of the service
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	no	In the EUCS these are both 03.2 not applicable without operation of the service
CS-03.3	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	no	In the EUCS these are both 03.2 not applicable without operation of the service
CS-03.4	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	no	not applicable without operation of the service
CS-03.5	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	no	not applicable without operation of the service
CS-03.6	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	partly	Done in the development and testing phase Identify Vulernabilites in the System Evaluate impact of vulnerabilities to our system Mitigate or resolve the resulting risks
CS-03.7	The CSP shall protect all SIEM logs to avoid tampering	Substantial	no	not applicable without operation of the service

CS-04.1	Each network perimeter shall be controlled by security gateways	Basic	no	not applicable without operation of the service
CS-04.2	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows	Substantial	no	not applicable without operation of the service
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	no	not applicable without operation of the service
CS-04.4	Each network perimeter shall be controlled by redundant and highly available security gateways	High	no	not applicable without operation of the service
CS-04.5	The CSP shall automatically monitor the control of the network perimeters to guarantee fulfilment of CS-04.1	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service
CS-05.2	The CSP shall logically or physically separate the networks for administration from the CSCs' networks	Basic	no	not applicable without operation of the service
CS-05.3	The CSP shall segregate physically or logically the networks used to migrate or create virtual machines	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
CS-06.1	The CSP shall define, document and implement segregation mechanisms at network level the data traffic of different cloud customers	Basic	no	not applicable without operation of the service
CS-06.2	When implementing of infrastructure capabilities, the secure segregation shall be ensured by physically separated networks or by strongly encrypted VLANs	High	no	not applicable without operation of the service

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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
CS-07.4	The CSP shall perform a full review of the network topology documentation at least once a year	Substantial	no	not applicable without operation of the service
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		not applicable without operation of the service
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		not applicable without operation of the service
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		not applicable without operation of the service
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	partly	TLS

CS-09.2	The policy and procedures shall include references to the classification of assets (cf. AM-05)	Substantial	no	CS-09.1 can be partly prepared by us, but as we do not implement the policies and procedures, this documentation is not possible

Ref	Description	Ass. Level	Applicable	Comment
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	yes	Document the respective interfaces in the archtiecture documentation
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	yes	
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	yes	OIDC and TLS
PI-01.4	Communication over untrusted networks shall be encrypted according to CKM-02	Basic	yes	TLS
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
PI-03.2	The CSC's data deletion shall include metadata and data stored in the data backups as well	Basic	no	not applicable without operation of the service
PI-03.3	The cloud customer's data deletion procedures shall prevent recovery by forensic means	Substantial	no	not applicable without operation of the service
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	no	not applicable without operation of the service
PI-03.5	At the end of the contract, the CSP shall delete the technical data concerning the client	Substantial	no	not applicable without operation of the service

Ref	Description	Ass. Level	Applicable	Comment
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	no	No Change Management in the Development phase
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	no	
CCM-02.1	The CSP shall categorize and prioritize changes considering the potential security effects on the system components concerned	Basic	no	
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	no	
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	no	

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	no
CCM-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	no
CCM-03.1	The CSP shall test proposed changes before deployment	Basic	no
CCM-03.2	The type and scope of the tests shall correspond to the risk assessment	Substantial	no
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	no
CCM-03.4	In accordance with contractual requirements, the CSP shall involve CSCs into the tests.	Substantial	no
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	no
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	no
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	no
CCM-03.8	The CSP shall document and implement a procedure that ensures the integrity of the test data used in pre-production	High	no

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	no
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	no
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	no
CCM-04.2	The CSP shall involve CSCs in the approval process according to contractual requirements	Substantial	no
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	no
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	no
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	no
CCM-05.3	The CSP shall automatically monitor changes in the production environment to guarantee fulfilment of CCM-05.1	High	no
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	no

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	no
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	no

Ref	Description	Ass. Level	Applicable	Comment
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	yes	Document the security processes in development (SCA, SAST, etc)
DEV-01.2	The policies and procedures for secure development shall consider information security from the earliest phases of design	Basic	yes	document the threat modeling in the security concept
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	partly	Secure Conding standards were adhered to
DEV-01.4	The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools	Substantial	yes	Procedures followed while developing the system E.g. useage of SAST/SCA/etc tools in development, code review based on OWASP Top 10 Vulnerabilities
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	partly	SCA - DependencyCheck

DEV-02.2	The CSP shall document and implement policies for the use of third-party and open source software	Substantial	yes	Part of the Security Concepts E.G. we only used activly maintained open source software components
DEV-02.3	The CSP makes its list of dependencies available to customers upon request	Substantial	no	
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	partly	Security Consideration for all dependencies are taken into account
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	partly	This is an Open Source Project, so only the integrity is of interest
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	yes	git
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	yes	ECO will provide a secure test environment the development env is run locally on the development machines
DEV-03.4	The CSP shall consider the development and test environments when performing risk assessment	Substantial	no	not applicable without operation of the service
DEV-03.5	The CSP shall include development resources as part of the backup policy	Substantial	no	not applicable without operation of the service
DEV-04.1	The CSP shall ensure that production environments are physically or logically separated from development, test or pre-production environments	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service

DEV-04.3	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment	High	yes	Depends on ECO
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	yes	Test all implemented Security Mechanisms
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	yes	Documentation should contain input and output values, possible error codes of authentication service Run OIDC conformance test and document results.
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	yes	UnitTests of Auth Component Test through all possible input combinations
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	yes	Document the UnitTests
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	yes	Code coverage by UnitTest specifically for the code responsible for the authentication
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	yes	SCA - DependencyCheck

DEV-06.2	The procedures for identifying vulnerabilities shall be integrated in the development process.	Basic	yes	This is handled by the Integration into the CI/CD pipeline
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	yes	Document the Security tooling and code review in the security concept
DEV-06.4	Code reviews shall be regularly performed by qualified personnel or contractors	High	yes	document code review procedure in security concept
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	yes	Found vulernabilities in the development phase are addressed immidiatly
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	no	not applicable without operation of the service

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	no	no outsourcing in the development phase
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	no	no outsourcing in the development phase
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	no	no outsourcing in the development phase
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	no	no outsourcing in the development phase

Ref	Description	Ass. Level	Applicable	Comment
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	partly	The used open source components are monitored für vulnerabilities while the system is in development
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	partly	Vulnerabilities found in dependencies are adressed
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	no	No subservice organizations

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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations

PM-02.5	The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually	Basic	no	No subservice organizations
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	no	No subservice organizations
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; Description of the service; * Classification based on the risk assessment; * Beginning of service usage; and * Proof of compliance with contractually agreed requirements.	Substantial	no	No subservice organizations
PM-03.3	The CSP shall verify the directory for completeness, accuracy and validity at least annually	Basic	no	No subservice organizations
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	no	No subservice organizations

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	no	No subservice organizations
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	no	No subservice organizations
PM-04.4	Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf. RM-01)	Basic	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations

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	no	No subservice organizations
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	no	No subservice organizations
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	no	No subservice organizations

Ref	Description	Ass. Level	Applicable	Comment
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IM-01.3	The CSP shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents	Basic	no	not applicable without operation of the service
IM-01.4	The CSP shall inform the customers affected by security incidents in a timely and appropriate manner	Substantial	no	not applicable without operation of the service
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	partly	This can be prepared by us, see Asset documentation for storage location of data
IM-01.6	The incident management policy shall include analysis plans for typical security incidents	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IM-02.5	The CSP shall monitor the processing of incident to verify the application of incident management policies and procedures	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IM-03.2	The CSP shall make information on security incidents or confirmed security breaches available to all affected customers	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IM-03.4	The CSP shall allow customers to actively approve the solution before automatically approving it after a certain period	High	no	not applicable without operation of the service
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	no	not applicable without operation of the service

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	no	not applicable without operation of the service
IM-04.3	The CSP shall define, make public and implement a single point of contact to report security events and vulnerabilities	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
IM-06.2	The CSP shall only contract supporting external bodies that are qualified incident response service providers or government agencies	Basic	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

IM-07.1	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents	Basic	no	not applicable without operation of the service
IM-07.2	The documents and evidence shall be archived in a way that could be used as evidence in court	Substantial	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service
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	no	not applicable without operation of the service

Ref	Description	Ass. Level	Applicable	Comment
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
BC-01.3	The business continuity and contingency management process owner shall ensure that sufficient resources are made available for an effective process	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
BC-04.3	The tests shall involve CSCs and relevant third parties, such as external service providers and suppliers	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

Ref	Description	Ass. Level	Applicable	Comment
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	no	not applicable without operation of a company providing this service
CO-01.2	The CSP shall document and implement procedures for complying to these contractual requirements	Substantial	no	not applicable without operation of a company providing this service
CO-01.3	The CSP shall provide these procedures when requested by a CSC	High	no	not applicable without operation of a company providing this service
CO-01.4	The CSP shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the service	High	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
CO-02.3	The CSP shall grant its CSCs contractually guaranteed information and define their audit rights	High	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
CO-03.2	The internal audit shall check the compliance with the requirements of the scheme at the targeted EUCS assurance level.	Basic	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
CO-03.4	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions	High	no	not applicable without operation of a company providing this service
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	partly	This can be prepared by selecting security scanning tools and establishing a baseline for the security monitoring
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	no	not applicable without operation of a company providing this service
CO-03.7	The CSP shall inform CSCs who operate an EUCS-certified cloud service of nonconformities relatively to EUCS requirements	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service

Ref	Description	Ass. Level	Applicable	Comment
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	yes	
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	yes	
DOC-01.3	The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use	Basic	yes	
DOC-01.4	The CSP shall describe in the user documentation all risks shared with the customer	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
DOC-02.3	The presentation of the vulnerabilities shall follow an industry-accepted scoring system for the description of vulnerabilities	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
DOC-04.2	If the CSP claims compliance to security profiles for its cloud service, the justification shall cover the security profiles.	Basic	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
DOC-04.4	The justification shall be based on a risk analysis according to RM-01	Substantial	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
DOC-05.3	The CSP shall make the documentation defined in DOC-05.1 available to cloud customers upon request	Basic	no	not applicable without operation of a company providing this service

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	no	not applicable without operation of a company providing this service
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	no	not applicable without operation of a company providing this service
DOC-06.2	The CSP shall make the documentation defined in DOC-06.1 available to cloud customers upon request	Basic	no	not applicable without operation of a company providing this service
DOC-06.3	The CSP shall justify the contributions in a companion document	Substantial	no	not applicable without operation of a company providing this service