MALTA DIGITAL INNOVATION AUTHORITY

TAAF Control Objectives

Document for Public Consultation

Contents

1 Public Consultation

This document is presented to obtain feedback from stakeholders prior to finalisation of the document.

The fees associated with TAAF are being published in a separate document as part of this public consultation exercise.

These draft TAAF Guidelines ('the Guidelines') are being published by the MDIA for consultation strictly in relation to the subject matter of technology assurance.

The laws governing the MDIA and innovative technology are currently going through a re-drafting exercise. These draft TAAF Guidelines that are being consulted on make reference to laws which are currently being amended as though such amendments have already entered into force. Applicable legislation may change further by the time the Guidelines are published in their final format. Such amendments may introduce modifications that affect the contents of this technical document. Once the amendments come into force, this document may be revised, amended, or updated accordingly to ensure compliance and alignment with the updated legal framework.

Any feedback must be submitted to the MDIA on taaf@mdia.gov.mt by the 30th June 2023.

Malta Digital Innovation Authority

19th May 2023

2 TAAF Control Objectives

The Technology Assurance Assessment (TAAF) Framework Control Objectives document presents the complete set of controls related to the framework.

This document is primarily intended for Assessors but may also be of interest to potential Applicants to review the controls they will be assessed against.

> *Note: This document is meant to accompany the TAAF Guidelines document. Please make sure you are familiar with the TAAF Guidelines first before reviewing this document.*

2.1 TAAF Summary

TAAF provides a flexible framework for Assurance of technological products or services.

The Control Objectives applicable to the Applicant depend on the Applicant's selection of three (3) key criteria as part of the application process:

1. Assessment Level
2. Technology Domains
3. Control Types

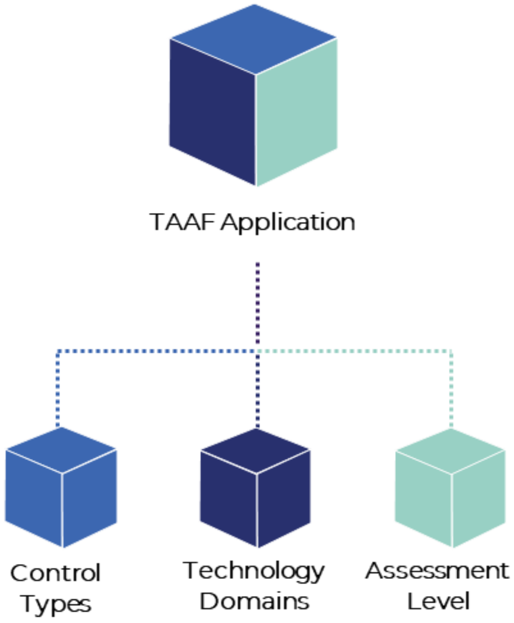

Figure 1 The 3 key components of a TAAF Application

2.1.1 TAAF Assessment Levels

The Assessment Level determines the type of recognition to be issued by the MDIA and how onerous the controls to be assessed against are.

The Assessment Level also determines the type of Assessment that needs to be carried out to satisfy the MDIA's TAAF requirements, as well as the type of Assessor.

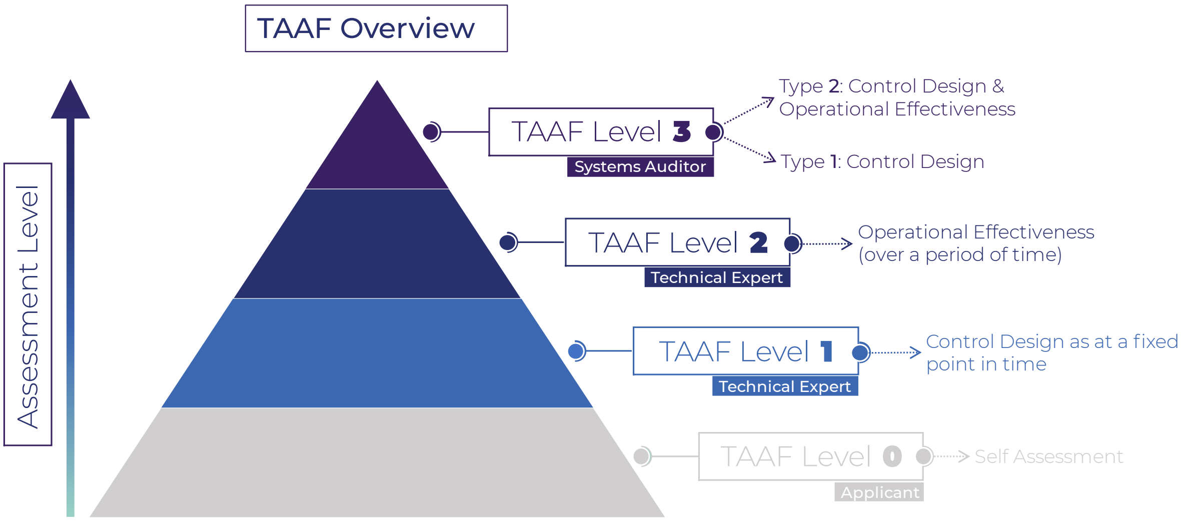

Figure 2 - an overview of the TAAF Assessment Levels

> *Note: This document does not apply to TAAF Assessment Level 0, since Self-Assessments are domain specific, and will each be governed by specific procedures and controls.*

2.1.2 Technology Domains

TAAF provides controls for five (5) Technology Domains. The Applicant must identify the relevant Technology Domains at application stage.

These are:

1. **General Innovative Technologies**
2. **Cloud Computing**
    a. For Cloud Infrastructure Users; or
    b. For Cloud Infrastructure Providers.
3. **Internet of Things (IoT)**
4. **Artificial Intelligence (AI)**
5. **Distributed Ledger Technologies (DLT)**

2.1.3 Control Types

As part of the application process, the Applicant must also identify which Control Types are relevant to them and their IDPS, as each Technology Domain provides control types relevant to different categories of controls.

These are:

1. **Accountability**
2. **Availability**
3. **Confidentiality**
4. **Integrity**
5. **Privacy**

3 Selecting the relevant Control Objectives

While this document presents all the control objectives that may make up TAAF, there are a significant number of possibilities, all depending on what the Applicant's selected as their Assessment criteria at application stage.

The controls applicable to an IDPS are depending on the Technology Domain, Assessment Level, and Control Types identified.

This document presents all the control objectives for each Technology Domain, further categorised by Control Objective Domains, and separated by the respective Assessment Level they pertain to. In each control, the applicable Control Types are also listed.

Note that due to the permutations possible, some control objectives between Technology Domains may overlap. In this case the control objective is only deemed to be applicable one time for reporting purposes.

4 General Innovative Technology Controls

The General Innovative Technology Controls refer to on-premises computing systems and services, including servers, storage, databases, networking, software, analytics, and automation.

4.1 TAAF Level 1

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the on premises infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a risk assessment methodology to be followed on its on premises infrastructure. The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the on premises service and are in the area of responsibility of the applicant: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the system components.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall stay informed about current threats and vulnerabilities via a documented Threat Modelling process.

Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall have a documented an Information Security Policy/ process/ guidelines that outlines the need to include information security in the project management of all projects that may affect the service, regardless of the nature of the project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document a global Information Security policy covering at least the following aspects: i) the importance of information security, based on the requirements of on premises infrastructure in relation to information security, as well as on the need to ensure the security of the information processed and stored by the applicant and the assets that support the services provided; ii) the security objectives and the desired security level, based on the business goals and tasks of the applicant; iii) the commitment of the applicant to implement the security measures required to achieve the established security objectives; iv) the most important aspects of the security strategy to achieve the security objectives set; and v) the organisational structure for information security in the ISMS application area. The applicant's top management shall approve and endorse its global information security policy. The applicant shall communicate and make available the global information security policy to internal and external employees and to on premises service customers, in the case the applicant is a on premises service provider.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including: i) Objectives; ii) Scope; iii) Roles and responsibilities within the organization; v) Steps for the execution of the security strategy; vi) Applicable legal and regulatory requirements; The applicant shall communicate and make available the policies and procedures to all internal and external employees.

Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall maintain a list of exceptions which are limited in time to the security policies and procedures, including associated controls. The list of exceptions shall be reviewed at least annually.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall document, communicate and implement information handling policies and procedures to protect the lifecycle of information in the organisation.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall document, communicate and implement information/ data classification polies and procedures to enforce appropriate safeguard and controls as per the confidentiality of data.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document risk management policies and procedures for the following aspects: i) Identification of risks associated with the loss of confidentiality, integrity, availability (CIA triad); ii) authenticity of information within the scope of the ISMS and assigning risk owners iii) Analysis of the probability and impact of occurrence and determination of the level of risk; iv) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; v) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and vi) Documentation of the activities implemented to enable consistent, valid and comparable results.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall implement the policies and procedures covering risk assessment on the entire perimeter of the on premises infrastructure. The applicant shall make the results of the risk assessment available to relevant stakeholders.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the maintenance of its on premises infrastructure in the production environment, and all positions with access to customer data and system components. The applicant shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: i) Verifying whether a violation has occurred; and ii) Consideration of the nature and severity of the violation and its impact. If disciplinary measures are defined in the policy, then the internal and external employees of the applicant shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity of all internal and external employees of the applicant with access to customer data or system components under the applicant's responsibility, or who will have access in the production environment shall be reviewed before commencement of employment in a position.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures. The applicant shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the on premises infrastructure, even if anonymised and decontextualized.

The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a security awareness and training program that covers basic Information Security principles such as but not limited to: i) Handling system components used in the production environment in accordance with applicable policies and procedures; ii) Handling data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; iii) Information about the current threat situation; and iv) Correct behaviour in the event of security incidents. The applicant shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define specific policies/ procedures that communicates to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed. The applicant shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall define an Asset Management Policy for maintaining an inventory of assets.

Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The applicant shall document, communicate and implement policies and procedures for acceptable use and safe handling of assets.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The applicant shall document, communicate and implement a procedure for the commissioning of hardware in the production environment, based on applicable policies and procedures. This procedure mentioned shall include the complete and permanent deletion of the data or the proper destruction of the media.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant shall a procedure/ process that shall include steps to ensure that all assets under custody of an employee are returned upon termination of employment.
Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	The applicant shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits.
Physical Security		

Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The applicant shall document, communicate and implement policies and procedures related to the physical access control to the security areas. The access control policy shall require at least one authentication factor for accessing any non-public area. The access control policy shall describe the physical access control derogations in case of emergency. The applicant shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters. The applicant shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall document, communicate, and implement policies and procedures concerning work in non-public areas.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning the Physical Security controls and safeguards in place. The applicant shall use encryption on removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media.
On premises data centres, are protected against external and environmental threats.	Integrity / Availability	The applicant shall document and communicate and implement policies and procedures outlining security requirements related to external and environmental threats, addressing the following risks in accordance with the applicable legal and contractual requirements: i) Faults in planning ii) Unauthorised access iii) Insufficient surveillance iv) Insufficient air-conditioning v) Fire and smoke vi) Water vii) Power failure viii) Air ventilation and filtration

Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.
Policies are defined that ensure the protection against malware of IT equipment related to the on premises service.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures to protect its systems and its customers from malware, covering at least the following aspects: i) Use of system-specific protection mechanisms ii) Operating protection programs on system components under the responsibility of the applicant that are used to provide the on premises service in the production environment iii) Operation of protection programs for employees' terminal equipment
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall deploy malware protection, if technically feasible, on all systems that support the on premises infrastructure e in the production environment, according to policies and procedures.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for data backup and recovery.
Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the logging and monitoring of events on system components.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the secure handling of derived data.
Log data can be unambiguously attributed to a on premises customer.	Integrity / Privacy / Accountability	The log data generated allows an unambiguous identification of user accesses at the customer level to support analysis in the event of an incident.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	Changes to the logging and monitoring configuration are made in accordance with applicable policies.

Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with respect to incident handling measures.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement general guidelines with respect to hardening on premises infrastructure components.
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make access policies and procedures for controlling access to information resources and based on the business and security requirements of the applicant, in which at least the following aspects are covered: i) Parameters to be considered for making access control decisions ii) Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle. iii) Use of a role-based mechanism for the assignment of access rights iv) Segregation of duties between managing, approving and assigning access rights v) Dedicated rules for users with privileged access vi) Requirements for the approval and documentation of the management of access rights. The applicant shall link the access control policy with the physical access control policy, to guarantee that the access to the premises where information is located is also controlled.

Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document policies for managing accounts in which at least the following aspects are described: i) Assignment of unique usernames; ii) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type. The applicant 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. The applicant 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. The applicant shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the on premises service that comply with the role and rights concept and with the policies for managing accounts.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement general guidelines with respect to user access review/ recertification.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The applicant shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: i) The selection of mechanisms suitable for every type of account; ii) The protection of credentials used by the authentication mechanism; and iii) The generation and distribution of credentials for new accounts.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: i) Non-reuse of credentials; ii) Recommendations for renewal of passwords; iii) Rules on the required strength of passwords, together with mechanisms to communicate and enforce the rules; and iv) Rules on storage of passwords; Passwords shall be only stored using cryptographically strong hash functions.
Cryptography and Key Management		

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall document, communicate, and implement policies and procedures that include technical and organizational safeguards for encryption and key management in which at least the following aspects are described: i) Usage of strong encryption procedures and secure network protocols ii) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys iii) Consideration of relevant legal and regulatory obligations and requirements
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The applicant shall document and implement procedures and technical safeguards to encrypt customers' data during storage.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	Procedures and technical safeguards for secure key management shall be defined and followed by the applicant.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures outlining technical safeguards and guidelines that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement specific security requirements aligned within its network security policy.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	The applicant shall define, document and implement policies and procedures outlining segregation mechanisms at network level to separate data traffic of different customers.

A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The applicant shall maintain up-to-date all documentation of the logical structure of the network.
Change and Configuration Management		
Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The applicant shall document, implement, and communicate policies and procedures for change management of the IT systems supporting the on premises infrastructure.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are performed by authorized accounts.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures according to the technical and organisational measures for the secure development of the on premises infrastructure. The policies and procedures for secure development shall consider information security from the earliest phases of design.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall document and implement policies for the use of third-party and open source software.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.

The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure the separation of pre-production and production environments.
Appropriate measures are taken to identify vulnerabilities introduced in the on premises service during the development process.	Confidentiality / Integrity / Availability	The applicant shall define appropriate safeguards or guidelines to check the on premises service for vulnerabilities that may have been integrated into the on premises service during the development process. The procedures for identifying vulnerabilities shall be integrated in the development process.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	When outsourcing development of the on premises infrastructure or components thereof to a contractor, the applicant shall document, communicate and implement Third Party policies or procedures that address the security requirements of the outsourced software.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the on premises infrastructure/ service. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the on premises infrastructure/ service. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the on premises service.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures according technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant 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

Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement a procedure to archive all documents and evidence that provide details on security incidents The applicant 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.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for establishing the strategy and guidelines to ensure business continuity and disaster recovery and contigency management.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The applicant shall document, communicate and implement policies and procedures for performing a business impact assessment to determine the impact of any malfunction to the on premises infrastructure.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The applicant shall document, communicate and implement a business continuity plan and disaster recovery plan to ensure continuity of the services, taking into account information security constraints and the results of the business impact assessment. The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the on premises service.

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the on premises service.	Privacy	The applicant shall document, communicate, make available and implement policies and procedures for planning and conducting audits and addressing at least the following aspects: i) Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; ii) Activities that may result in malfunctions to breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and iii) Logging and monitoring of activities.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control systems. The internal audit shall check the compliance with respect to their ISMS and regulatory frameworks. The applicant shall document specifically deviations that are nonconformities from their ISMS and regulatory frameworks including an assessment of their severity, and keep track of their remediation.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall define, communicate and implement policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall define, communicate and implement a Privacy policy outlining the entity's objectives related to confidentiality and how confidential data are maintained. The Privacy Policy is reviewed and updated at least on an annual basis.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The Applicant is shall define, communicate and implement policies and procedures to safeguard, protect, process and retain personal data.

4.2 TAAF Level 2

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's ISMS shall be based in accordance to ISO/IEC 27001.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the on premises infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the applicant's on premises infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the on premises service, regardless of the nature of the project.
Information Security Policies		

The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions shall be subjected to the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over the applicable controls that correspond to the data handling policies and procedures, which should include controls for all data life cycle phases: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall classify all data according to the data classification policies and procedures on both structured and unstructured data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place.

DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to external storage devices are monitored and prevented for certain categories of sensitive data. Most sensitive data types are monitored.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of sensitive data assets. Data ownership has been defined for sensitive data elements.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their on premises infrastructure and monitor the remediation of the risks and revise the risk assessment results accordingly.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.

The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The extent of the competency and integrity review (screening) of all internal and external employees shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks. The competency and integrity of internal and external employees of the applicant shall be reviewed before commencement of employment in a position with a higher risk classification.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties. The applicant shall update their security awareness and training program at least annually. The applicant shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group. The applicant shall measure and evaluate the learning outcomes achieved through the awareness and training programme.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall monitor the effectiveness of the policies/ procedures that change/ revoke accounts and logical access rights when the employment of an internal or external employee is terminated or changed. A checklist for the return/ change of assets should be followed by HR or the IT departments when the employment of an internal or external employee is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the applicant for the protection of confidential information and operational details. The agreements shall be accepted by external service providers and suppliers when the contract is agreed. The agreements shall be accepted by internal employees of the applicant before authorisation to access data of customers is granted.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	An asset inventory or asset Register shall be maintained and periodically updated by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle. The information recorded with assets shall include the measures taken to manage the risks associated to the asset and the data it contains throughout its life cycle.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The policies and procedures for acceptable use and safe handling of assets shall address at least the all aspects of the asset lifecycle as applicable to the asset.

The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The procedure shall ensure that the risks arising from the commissioning are identified, analysed and mitigated. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof. The procedure 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.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant 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. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to customer data, the production environment, or any component thereof.
Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. When applicable, the applicant shall label all assets according to their classification in the asset classification schema.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process customer data. The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay. The access control policy shall include logging of all accesses to non-public areas that enables the applicant to check whether only defined personnel have entered these zones.

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The policies and procedures shall include a clear screen policy and a clear desk policy for documents and removable media.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place.
On premises data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall be based on criteria which comply with established rules of technology. The applicant shall provide at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience. The applicant shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload. The applicant shall meet the requirements included in contractual agreements with customers regarding the provision of the on premises service in case of capacity bottlenecks or personnel and IT resources outages.
The capacities of critical resources such as personnel and IT resources are monitored.	Integrity / Availability	The applicant shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning for the IT resources.
Policies are defined that ensure the protection against malware of IT equipment related to the on premises service.	Confidentiality / Integrity / Availability	The applicant 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.
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	Signature-based and behaviour-based malware protection tools shall be updated at least daily.

Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the on premises operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted; and iii) Access to the backed-up data and the execution of restores is performed only by authorised persons.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall provide evidence on the operational effectiveness of monitoring their data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The restore tests shall assess if the specifications for the RTO and RPO agreed are met. Any deviation from the specification during the restore test shall be reported to the applicant's responsible person for assessment and remediation.
Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; and v) Time synchronisation of system components.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Purpose for the collection and use of derived data beyond the operation of the on premises service, including purposes related to the implementation of security controls; ii) Anonymisation of the data whenever used in a context that goes beyond a single customer; iii) Period of storage reasonably related to the purposes of the collection; iv) Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and v) Provision of the derived data to users according to contractual agreements; and vi) Automated event monitoring

The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation. Log data shall be deleted when it is no longer required for the purpose for which they were collected. 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. The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection.
Log data can be unambiguously attributed to a on premises customer.	Integrity / Privacy / Accountability	The applicant shall make available interfaces to conduct forensic analysis of infrastructure components and their network communication.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The applicant shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant 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.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Regular identification of vulnerabilities; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.

The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the on premises service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall perform the vulnerability scanning on all system components test at least once a month. The applicant 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, as identified in a risk analysis. The applicant shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall harden all the system components under their on premises infrastructure, according to accepted industry standards. The hardening requirements for each system component shall be documented.
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the effectiveness of access request policies and procedures for at least: i) Normal access requests; ii) Privileged access requests; iii) emergency access requests; and iv) external employees' access request
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts or two-moth inactivity. The limits on authentication attempts used in mechanism for user accounts under the responsibility of the applicant shall be based on the risks on the accounts, associated access rights and authentication mechanisms The applicant 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.

The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The review defined shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. The applicant handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. The applicant shall perform periodic access reviews on applications of medium/ high criticality rating on a bi-annual basis.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks. 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. The applicant shall require strong authentication for accessing the administration interfaces used by the applicant.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to all environments of the applicant shall be authenticated, including non-production environments. Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security The applicant shall offer strong authentication methods to the employees and on premises service's customers for use with the accounts under their responsibility.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	When creating credentials, compliance with specifications is enforced automatically as far as technically possible. The credential associated to a personal account should be changed on bi-monthly basis and when the credential is changed or renewed, the person associated to that account shall be notified. 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.
The assets in and around the on premises service are managed in a way that ensure that access restrictions are enforced between different categories of assets	Confidentiality / Integrity / Privacy / Accountability	The applicant shall timely inform a customer whenever internal or external employees of the applicant access in a non-encrypted form to the customer's data processed, stored or transmitted in the on premises service without the prior consent of the customer, including at least: i) Cause, time, duration, type and scope of the access; and ii) Enough details to enable subject matters experts of the customer to assess the risks of the access.
Cryptography and Key Management		

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) Strong cryptography and security protocols are used (e.g., TLS, IPsec, SSH, etc.) to safeguard confidential information during transmission over open, public networks.
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known only to the customer in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions. The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the customer.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	The applicant shall follow the following measures with respect to key management: i) Generation of keys for different cryptographic systems and applications; ii) Issuing and obtaining public-key certificates; iii) Provisioning and activation of the keys; iv) Secure storage of keys including description of how authorised users get access; v) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; vi) Handling of compromised keys; and vii) Withdrawal and deletion of keys.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant 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.

The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements within its network, including at least: i) when the security zones are to be separated and when the infrastructure is to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; and iii) how the data traffic for administration and monitoring are segregated from each other at the network level.
The communication flows within the on premises systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant shall distinguish between trusted and untrusted networks, based on a risk assessment. The applicant shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable). The applicant 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. The applicant 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.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows. The system access authorisation for cross-network access shall be based on a security assessment according to the requirements of the on premises infrastructure or customers.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by physically separated networks or by strongly encrypted VLANs.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The logical structure of the applicant's network 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 customers' data are stored.
Change and Configuration Management		

Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the documentation of changes in the system, operational and user documentation.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall define the testing scope prior to deployment. The applicant shall include safeguards that guarantee the confidentiality of the data during the whole process. The applicant 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.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall provide sufficient evidence on the obtained approvals that were gathered prior to deployment.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall define roles and rights for the authorised personnel or system components who are allowed to make changes to the on premises service in the production environment and also utilise version controls. All changes to the on premises service in the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall maintain a list of all third-party and open source software. In the case that the applicant provide on premises services, the list of dependencies of all third-parties and open source software shall be made available to customers upon request.

The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the on premises infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall ensure that production environments are physically or logically separated from development, test or pre-production environments. Data contained in the production environments shall not be used without data masking in development, test or pre-production environments in order not to compromise their confidentiality.
Appropriate measures are taken to identify vulnerabilities introduced in the on premises service during the development process.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the security safeguards that include but are not limited to the following aspects: i) Static Application Security Testing; ii) Dynamic Application Security Testing; iii) Code reviews by subject matter experts; and iv) Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own on premises service.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of contractual agreement regarding the development of the on premises infrastructure or components thereof by a third party serving the following aspects: i) Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; ii) Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and iii) Sufficient verifications are carried out to rule out the existence of known vulnerabilities.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the following aspects related to third party risk management: i) Requirements for the assessment of risks resulting from the procurement of third-party services; ii) Requirements for the classification of third parties based on the risk assessment by the applicant; iii) Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; iv) Information security awareness and training requirements for staff; v) Applicable legal and regulatory requirements; vi) Requirements for dealing with vulnerabilities, security incidents, and malfunctions; vii) Specifications for the contractual agreement of these requirements; viii) Specifications for the monitoring of these requirements.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties. The applicant 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. The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; and viii) Beginning of service usage.

Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall inform the customers affected by security incidents in a timely and appropriate manner. The applicant shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall maintain a catalogue (Incident Classification Matrix) that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents. 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. The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant 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. The applicant shall inform its customers about the actions taken, according to the contractual agreements. The applicant shall define, make public and implement a single point of contact to report security events and vulnerabilities
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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 The applicant shall only contract supporting external bodies that are qualified incident response service providers or government agencies.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The documents and evidence shall be archived in a way that could be used as evidence in court. When the applicant requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the applicant shall contract a qualified incident response service provider only.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business continuity and disaster recovery and contigency 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.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed on a periodic basis and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; and viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); The business impact analysis resulting from these policies and procedures shall be reviewed at least once a year, or after significant organisational or environment related changes.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be periodically performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of on premises infrastructure components and services and alignment with customers); vi) Methods for putting the plans into effect; and The business continuity plan shall be reviewed at least once a year, or after significant organisational or environment-related changes.
Compliance		

The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document and implement procedures and measure its effectiveness for complying to these contractual requirements.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the on premises service.	Privacy	The applicant 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.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked. The applicant shall inform customers for potential deviations and identified vulnerabilities.
Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow any customers to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall provide evidence on the followed policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall ensure that the Privacy policy is signed by all new internal and external employees upon onboarding. The applicant shall provide evidence for all controls in place that are applicable to the regulatory Data Protection requirements.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; and iii) secure disposal of personal data according to the regulatory Data Protection requirements.

4.3 TAAF Level 3

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall have obtained a valid ISO/IEC 27001 certification.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the on premises infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the on premises infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions. The applicant shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain a list with the competent authorities in terms of information security and relevant technical groups on an bi-annual basis to stay informed about current threats and vulnerabilities that are specific to their sector.

Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the on premises service, regardless of the nature of the project. The applicant shall include the review and signoff from the Information Security Officer, prior to the initiation of a new project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least annually. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. The applicant's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of the on premises infrastructure. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees. Policies and procedures updates are communicated internally through different notification channels.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions to a security policy or procedure shall be approved by the top management or the Information Security Officer or at least a body who approved the security policy or procedure. The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over applicable controls that correspond to the handling policies and procedures, which should include specific for all data life cycle phases according to the data classification policies and procedures: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.

Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall use data labelling tool, which shall be consistently performed across most BUs for sensitive, unstructured data in accordance with data classification policies. Approved storage locations have been identified and configured for automatic data labelling as per the data classification policies and procedures, whilst data tagging is not performed on legacy data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place. The applicant shall enforce a solution that will allow expand the discovery capabilities of sensitive data on sanctioned third party cloud apps.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to storage devices are logged and prevented or owned based on the content of the information being transferred. A periodic review of the rules is conducted to update the rules to monitor and prevent new data types.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of information assets is maintained and assets are classified by the type of data contained and the relative risk. The inventory management is automated via the use of a centralized dashboard of a discovery tool.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels. The Risk Management Register should be updated at least on an annual basis.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their on premises infrastructure and monitor the remediation of the risks and revise the risk assessment results via an automated dashboard or risk compliance solution.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans. The applicant shall monitor the effectiveness of the risk treatment activities via an automated dashboard or risk compliance solution.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties. The applicant should provide evidence of employees' Information Security training on unacceptable behaviour or insider threat cases.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity review (screening) of internal and external employees of the applicant shall be conducted for the employees in all positions.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant’s code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The verification of the acknowledgement of information security policies and procedures shall be automatically monitored by the applicant. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to this.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the security awareness and training program. The applicant shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme. The applicant shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long. Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the logical access rights of users and assets of internal or external employees.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall periodically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers. More specifically, the requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly. The applicant shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall automatically monitor the asset inventory via the provisioning of an inventory tool to ensure that all entries on the inventory are up-to-date.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use. Exception forms should be used for requesting the use of removable media. Specific training and awareness modules with mandatory attendance should be in place for all internal and external employees with respect to safe handling of assets.

The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The approval of the commissioning and decommissioning of hardware shall be automatically monitored. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant 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. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. The requirements for sufficient asset protection shall be determined by the individuals or groups responsible for the assets (asset owners) and the Information Security Officer.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users The logging of accesses shall be automatically monitored and reviewed on an annual basis.

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area. The applicant shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place. The applicant shall ensure that any back-up equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted or has been destroyed beforehand using a secure deletion mechanism.
On premises data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime. The security requirements for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning.
The capacities of critical resources such as personnel and IT resources are monitored.	Integrity / Availability	The applicant shall make available to the customer the relevant information regarding capacity and availability on a self-service portal. The provisioning and de-provisioning of the IT resources shall be automatically monitored.
Policies are defined that ensure the protection against malware of IT equipment related to the on premises service.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces. The applicant shall update the anti-malware products at the highest frequency that the vendors actually offer.

Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms. The applicant shall automatically monitor the antimalware full scans to track detected malware or irregularities on a daily basis.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the on premises operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted, state-of-the-art form; iii) Access to the backed-up data and the execution of restores is performed only by authorised persons; and iv) Tests of recovery procedures.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall configure a portal for automatically monitoring their scheduled data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The applicant shall inform the on premises service customers or users, at their request, of the results of the recovery tests. Recovery tests shall be aligned with applicant's business continuity management requirements.
Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions to ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; v) Time synchronisation of system components; and vi) Compliance with legal and regulatory frameworks. The Applicant shall implement a centralized logging repository mechanism hosted in Malta that is available 24/7 relevant to the on-premises infrastructure.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments. The applicant shall automatically monitor that event detection is effective on the list of critical assets.

The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection. The applicant shall automatically monitor the aggregation and deletion of logging and monitoring data.
Log data can be unambiguously attributed to a on premises customer.	Integrity / Privacy / Accountability	In the context of an investigation of an incident concerning a on premises service customer, the applicant shall have the ability to provide to the customer the logs related to its service.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The access to system components for logging and monitoring shall require strong authentication.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant shall design the system components for logging and monitoring in such a way that the overall functionality is not restricted if individual components fail.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Automated identification of vulnerabilities through a commercial tool; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.

The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the on premises service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	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 threat landscape. Some of the penetration tests performed each year shall be performed by external service providers. The applicant 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 on premises systems. The applicant shall correlate the possible exploits of discovered vulnerabilities with previous incidents to identify if the vulnerability may have been exploited before its discovery.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall quarterly perform and review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the system components according to the appropriate hardening specifications.
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the use of an automated ticketing tool that supports all user access requests.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall provide a sample of privileged users access rights to validate that no toxic combinations are present with reference to the Segregation of Duties Matrix. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.

Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall implement the process on all user accounts under its responsibility. The applicant shall automatically monitor the implemented automated mechanisms. The applicant shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall perform the user access rights via the use of an automated access review/ recertification tool.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	The applicant must revise every six (6) months the list of employees who are responsible for a technical account within its scope of responsibility. The applicant shall maintain an automated inventory of the user accounts under its responsibility that have privileged access rights.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to the production environment of the applicant shall require strong authentication. The access to all environments of the applicant containing data shall require strong authentication.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant 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. Passwords of administrator accounts should be stored on logical key vaults.

The assets in and around the on premises service are managed in a way that ensure that access restrictions are enforced between different categories of assets	Confidentiality / Integrity / Privacy / Accountability	The applicant shall separate the administration interfaces made available to customers from those made available to its internal and external employees, and in particular: i) The administration accounts under the responsibility of the applicant shall be managed using tools and directories that are separate from those used for the management of user accounts under the responsibility of the customers; ii) The administration interfaces made available to customers shall not allow for any connection from accounts under the responsibility of the applicant; and iii) The administration interfaces used by the applicant shall not be accessible from the public network and as such shall not allow for any connection from accounts under the responsibility of the customer. The applicant shall require prior consent from a customer before any access in a non-encrypted form to the customer's data processed, stored or transmitted in the on premises service, providing meaningful information.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) All data should implement strong encryption mechanisms for their transmission (in transit).
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known exclusively by the customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	For the secure storage of keys and other secrets used for the administration tasks, the applicant shall use designated key vaults and should rotate the keys on a quarterly basis.
Communication Security		

The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network. The applicant shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements to connect within its network, including at least: i) when the security zones are to be separated and when the customers are to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; iii) how the data traffic for administration and monitoring are segregated from each other at the network level; iv) what internal, cross-location communication is permitted; and v) what cross-network communication is allowed.
The communication flows within the on premises systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant 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. The applicant shall assess the risks of identified vulnerabilities in accordance with the risk management procedure and follow-up measures shall be defined and tracked. The applicant shall protect all SIEM logs to avoid tampering.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Each network perimeter shall be controlled by redundant and highly available security gateways. The applicant shall automatically monitor the control of the network perimeters.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by usage of network addressing schemes or by strongly encrypted VLANs.

A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	In the case of an applicant providing on premises services, the logical structure of network documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions. The applicant shall perform a full review of the network topology documentation at least once a year.
Change and Configuration Management		
Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the proper information of on premises service customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; v) Requirements for the documentation of changes in the system, operational and user documentation; and vi) Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The tests performed any change before its deployment shall include tests on both a development environment, as well as testing environment. The applicant shall document and implement a procedure that ensures the integrity of the test data used in pre-production. The applicant shall perform penetration testing on components that are internet-facing. Before deploying changes on a system component, the applicant shall perform regression testing on other components of the on premises infrastructure that depend on that system component to verify the absence of undesirable effects. The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.

Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall automatically monitor the logs changes in the production environment to ensure that the principle of non-repudiation is maintained.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices via automated static or dynamic scanning tools.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall perform a risk assessment in accordance to Risk Management policies and procedures for every third party or open source software product.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the on premises infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The documentation of the tests of the security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test. The applicant shall consider the development and test environments when performing risk assessment. The applicant shall include development resources as part of the backup policy.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment.
Appropriate measures are taken to identify vulnerabilities introduced in the on premises service during the development process.	Confidentiality / Integrity / Availability	Code reviews shall be regularly performed by qualified personnel or contractors. The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts.

Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall 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. Internal or external employees of the applicant shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant 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. The reports shall include the complementary subservice organisation controls that are required, together with the controls of the applicant.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence over the organisation's third party management capabilities including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: i) Protection needs regarding the confidentiality, integrity and availability of information processed, stored, or transmitted by the third party; ii) Impact of a protection breach on the provision of the outsourcing service; iii)The applicant's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; vii) Security requirements; viii) Beginning of service usage; and ix) Proof of compliance with contractually agreed requirements.

Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall test the Incident Response Plan/ procedure at least on an annual basis.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall simulate the identification, analysis, and defence of security incidents and attacks on a quarterly basis through appropriate Table-top tests and exercises. The applicant shall review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness. The applicant shall monitor the processing of incident to verify the application of incident management policies and procedures.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow customers to actively approve the solution before automatically approving it after a certain period.
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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. 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The service provider shall establish an integrated team of forensic/ incident responder personnel specifically trained on evidence preservation and chain of custody management.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business business continuity and disaster recovery and contigency management and form a Business Continuity Management & Disaster Recoevry team, which is responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. The business continuity and disaster recovery and team shall ensure that sufficient resources are made available for an effective process.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed at least annually and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); ix) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and x) Estimation of the resources needed for resumption. The business impact analysis resulting from these policies and procedures shall be conducted and reviewed at regular intervals, at least once a year, or after significant organisational or environment related changes.

A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be at least annually performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of on premises infrastructure components and services and alignment with customers); vi) Methods for putting the plans into effect; vii) Continuous process improvement; and viii) Interfaces to Security Incident Management. The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall provide these procedures when requested by a customer. The applicant shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the service.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the on premises service.	Privacy	The applicant shall grant its customers contractually guaranteed information and define their audit rights.

Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions. The applicant shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate applicant's subject matter experts for immediate assessment and action.
Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow the customer to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. All commitments regarding locations of data processing and storage shall be enforced by the cloud service architecture.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall track the data request process via a ticketing system.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall document and implement an active monitoring tool of the regulatory Data Protection requirements they need to follow.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; iii) secure disposal of personal data according to the regulatory Data Protection requirements; iv) keeping a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.

5 Cloud Computing

Cloud Computing refers to the computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet (also defined as "the cloud").

*Note: * denotes controls that apply only to Cloud Infrastructure Providers. Controls marked with asterisk (*) do not apply to an IDPS that merely uses cloud services.*

5.1 TAAF Level 1

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes with respect to its infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes with respect to its cloud infrastructure.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a risk assessment methodology to be followed on its cloud infrastructure. The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the applicant: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the system components.

The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall stay informed about current threats and vulnerabilities via a documented Threat Modelling process.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall have a documented an Information Security Policy/ process/ guidelines that outlines the need to include information security in the project management of all projects that may affect the service, regardless of the nature of the project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document a global Information Security policy covering at least the following aspects: i) the importance of information security, based on the requirements of cloud infrastructure in relation to information security, as well as on the need to ensure the security of the information processed and stored by the applicant and the assets that support the services provided; ii) the security objectives and the desired security level, based on the business goals and tasks of the applicant; iii) the commitment of the applicant to implement the security measures required to achieve the established security objectives; iv) the most important aspects of the security strategy to achieve the security objectives set; and v) the organisational structure for information security in the ISMS application area. The applicant's top management shall approve and endorse its global information security policy. The applicant shall communicate and make available the global information security policy to internal and external employees and to cloud service customers, in the case the applicant is a cloud service provider.

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including: i) Objectives; ii) Scope; iii) Roles and responsibilities within the organization; v) Steps for the execution of the security strategy; vi) Applicable legal and regulatory requirements; The applicant shall communicate and make available the policies and procedures to all internal and external employees.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall maintain a list of exceptions which are limited in time to the security policies and procedures, including associated controls. The list of exceptions shall be reviewed at least annually.
Information Management		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall document, communicate and implement information handling policies and procedures to protect the lifecycle of information in the organisation.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall document, communicate and implement information/ data classification polies and procedures to enforce appropriate safeguard and controls as per the confidentiality of data.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall document risk management policies and procedures for the following aspects: i) Identification of risks associated with the loss of confidentiality, integrity, availability (CIA triad); ii) authenticity of information within the scope of the ISMS and assigning risk owners iii) Analysis of the probability and impact of occurrence and determination of the level of risk; iv) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; v) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and vi) Documentation of the activities implemented to enable consistent, valid and comparable results.

Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall implement the policies and procedures covering risk assessment on the entire perimeter of the cloud infrastructure. The applicant shall make the results of the risk assessment available to relevant stakeholders.
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the maintenance of its cloud infrastructure in the production environment, and all positions with access to customer data or system components. The applicant shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: i) Verifying whether a violation has occurred; and ii) Consideration of the nature and severity of the violation and its impact. If disciplinary measures are defined in the policy, then the internal and external employees of the applicant shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity of all internal and external employees of the applicant with access to customer data or system components under the applicant's responsibility, or who are responsible to provide the cloud service in the production environment shall be reviewed before commencement of employment in a position.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant used to provide the service in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures. The applicant shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the cloud infrastructure, even if anonymised and decontextualized.

The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a security awareness and training program that covers basic Information Security principles such as but not limited to: i) Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; ii) Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; iii) Information about the current threat situation; and iv) Correct behaviour in the event of security incidents. The applicant shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define specific policies/ procedures that communicates to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed. The applicant shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers.
Asset Management		

The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall define an Asset Management Policy for maintaining an inventory of assets.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The applicant shall document, communicate and implement policies and procedures for acceptable use and safe handling of assets.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the service in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	In case the applicant is a cloud service provider, the applicant shall document, communicate and implement a procedure for the commissioning of hardware in the production environment, based on applicable policies and procedures. This procedure mentioned shall include the complete and permanent deletion of the data or the proper destruction of the media.
The applicant's internal and external employees are probably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant shall a procedure/ process that shall include steps to ensure that all assets under custody of an employee are returned upon termination of employment.

Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	The applicant shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits.
Physical Security		
The buildings and premises related to the cloud service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises. *	Confidentiality / Integrity / Availability	The applicant shall define security perimeters in the buildings and premises related to the cloud service provided. The applicant shall define at least two security areas, with one covering all buildings and premises and one covering sensitive activities such as the buildings and premises hosting the information system for the production of the service.
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The applicant shall document, communicate and implement policies and procedures related to the physical access control to the security areas. The access control policy shall require at least one authentication factor for accessing any non-public area. The access control policy shall describe the physical access control derogations in case of emergency. The applicant shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters. The applicant shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning work in non-public areas.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning the Physical Security controls and safeguards in place. The applicant shall use encryption on removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media.

The premises from which the cloud service operated, and in particular its data centres, are protected against external and environmental threats. *	Integrity / Availability	The applicant shall document and communicate and implement policies and procedures outlining security requirements related to external and environmental threats, addressing the following risks in accordance with the applicable legal and contractual requirements: i) Faults in planning ii) Unauthorised access iii) Insufficient surveillance iv) Insufficient air-conditioning v) Fire and smoke vi) Water vii) Power failure viii) Air ventilation and filtration
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks. *	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.
Policies are defined that ensure the protection against malware of IT equipment related to the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures to protect its systems and its customers from malware, covering at least the following aspects: i) Use of system-specific protection mechanisms ii) Operating protection programs on system components under the responsibility of the applicant that are used to provide the cloud service in the production environment iii) Operation of protection programs for employees' terminal equipment
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall deploy malware protection, if technically feasible, on all systems that support the cloud infrastructure e in the production environment, according to policies and procedures.

Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for data backup and recovery.
Policies are defined to govern logging and monitoring events on system components under the applicant's responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the logging and monitoring of events on system components.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the secure handling of derived data.
Log data can be unambiguously attributed to a CSC. *	Integrity / Privacy / Accountability	The log data generated allows an unambiguous identification of user accesses at the cloud service customer level to support analysis in the event of an incident.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	Changes to the logging and monitoring configuration are made in accordance with applicable policies.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system cloud components.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with respect to incident handling measures.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement general guidelines with respect to hardening cloud infrastructure components.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make access policies and procedures for controlling access to information resources and based on the business and security requirements of the applicant, in which at least the following aspects are covered: i) Parameters to be considered for making access control decisions ii) Granting and modifying access rights based on the "least-privilege" principle and on the "need-to-know" principle. iii) Use of a role-based mechanism for the assignment of access rights iv) Segregation of duties between managing, approving and assigning access rights v) Dedicated rules for users with privileged access vi) Requirements for the approval and documentation of the management of access rights The applicant shall link the access control policy with the physical access control policy, to guarantee that the access to the premises where information is located is also controlled.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document policies for managing accounts in which at least the following aspects are described: i) Assignment of unique usernames; ii) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type. The applicant 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. The applicant 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. The applicant 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.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement general guidelines with respect to user access review/ recertification.

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The applicant shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: i) The selection of mechanisms suitable for every type of account; ii) The protection of credentials used by the authentication mechanism; and iii) The generation and distribution of credentials for new accounts.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: i) Non-reuse of credentials; ii) Recommendations for renewal of passwords; iii) Rules on the required strength of passwords, together with mechanisms to communicate and enforce the rules; and iv) Rules on storage of passwords; Passwords shall be only stored using cryptographically strong hash functions.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall document, communicate, and implement policies and procedures that include technical and organizational safeguards for encryption and key management in which at least the following aspects are described: i) Usage of strong encryption procedures and secure network protocols ii) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys iii) Consideration of relevant legal and regulatory obligations and requirements
The applicant has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage *	Confidentiality / Privacy	The applicant shall document and implement procedures and technical safeguards to encrypt cloud customers' data during storage.

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	Procedures and technical safeguards for secure key management shall be defined and followed by the applicant.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures outlining technical safeguards and guidelines that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement specific security requirements aligned within its network security policy.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks. *	Confidentiality / Integrity	The applicant shall define, document and implement policies and procedures outlining segregation mechanisms at network level to separate data traffic of different cloud customers.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The applicant shall maintain up-to-date all documentation of the logical structure of the network.
Portability and Interoperability		
Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems *	Confidentiality / Availability	The inbound and outbound interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.

Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems. *	Confidentiality / Privacy	The applicant shall implement procedures for deleting customers' data upon termination of their contract in compliance with the contractual agreements between them. The CSC's data deletion shall include metadata and data stored in the data backups as well.
Change and Configuration Management		
Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The applicant shall document, implement, and communicate policies and procedures for change management of the IT systems supporting the cloud infrastructure.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are performed by authorized accounts.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures according to the technical and organisational measures for the secure development of the cloud infrastructure. The policies and procedures for secure development shall consider information security from the earliest phases of design.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall document and implement policies for the use of third-party and open source software.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.

The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure the separation of pre-production and production environments.
Appropriate measures are taken to identify vulnerabilities introduced in the cloud service during the development process. *	Confidentiality / Integrity / Availability	The applicant shall define appropriate safeguards or guidelines to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process. The procedures for identifying vulnerabilities shall be integrated in the development process.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	When outsourcing development of the cloud infrastructure or components thereof to a contractor, the applicant shall document, communicate and implement Third Party policies or procedures that address the security requirements of the outsourced software.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the cloud infrastructure/ service. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the cloud infrastructure/ service. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the cloud service.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures according technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant 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

Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement a procedure to archive all documents and evidence that provide details on security incidents The applicant 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.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for establishing the strategy and guidelines to ensure business continuity and disaster recovery and contigency management.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The applicant shall document, communicate and implement policies and procedures for performing a business impact assessment to determine the impact of any malfunction to the cloud infrastructure.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The applicant shall document, communicate and implement a business continuity plan and disaster recovery plan to ensure continuity of the services, taking into account information security constraints and the results of the business impact assessment. The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference of the infrastructure.	Privacy	The applicant shall document, communicate, make available and implement policies and procedures for planning and conducting audits and addressing at least the following aspects: i) Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; ii) Activities that may result in malfunctions to breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and iii) Logging and monitoring of activities.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control systems. The internal audit shall check the compliance with respect to their ISMS and regulatory frameworks. The applicant shall document specifically deviations that are nonconformities from their ISMS and regulatory frameworks including an assessment of their severity, and keep track of their remediation.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall define, communicate and implement policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall define, communicate and implement a Privacy policy outlining the entity's objectives related to confidentiality and how confidential data are maintained. The Privacy Policy is reviewed and updated at least on an annual basis.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The Applicant is shall define, communicate and implement policies and procedures to safeguard, protect, process and retain personal data.
User Documentation		

Provide information to assist the customer in the secure configuration, installation and use of the cloud service. *	Confidentiality / Integrity / Availability / Privacy	The applicant shall make publicly available guidelines and recommendations to assist CSCs with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided. The applicant shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use.
Provide information to assist the customer in the secure configuration, installation and use of the cloud service *	Confidentiality / Integrity / Availability	The applicant shall operate or refer to a publicly available and daily updated online register of known vulnerabilities that affect the provided cloud customers.
Provide transparent information about the location of the data and of its processing	Confidentiality / Integrity / Privacy	The applicant shall provide comprehensible and transparent information on: i) Its jurisdiction; and ii) System component locations, including its subcontractors, where the cloud customer's data is processed, stored and backed up. The applicant shall provide sufficient information allowing clients to assess the suitability of locations that their data are stored from a legal and regulatory perspective.
Dealing with Investigation Requests from Government Agencies		
Cloud customers are kept informed of ongoing investigations if legally permitted. *	Privacy / Accountability	The applicant shall subject investigation requests from government agencies to a legal assessment by subject matter experts. The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken. The applicant shall inform the affected CSC(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service
Investigators only have access to the data required for their investigation after validation of the legality of their request. *	Privacy / Accountability	The applicant shall only provide access to or disclose cloud customer data in the context of government investigation requests after the applicant's legal assessment has shown that an applicable and valid legal basis exists and that the investigation request must be granted on that basis. The applicant shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate.

Product Safety and Security		
Cloud customers have access to sufficient information about the cloud service through error handling and logging mechanisms *	Integrity / Accountability	The applicant shall document, communicate and implement policies and procedures outlining product service safety and security safeguards and controls, which shall be offered to the CSCs.

5.2 TAAF Level 2

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes with respect to its infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's ISMS shall be based in accordance to ISO/IEC 27001.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the applicant's cloud infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special	Confidentiality / Integrity / Availability	The applicant shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.

interest groups. The information flows into the procedures for handling risks and vulnerabilities.		
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the cloud service, regardless of the nature of the project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions shall be subjected to the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated.
Information Management		

Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over the applicable controls that correspond to the data handling policies and procedures, which should include controls for all data life cycle phases: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall classify all data according to the data classification policies and procedures on both structured and unstructured data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to external storage devices are monitored and prevented for certain categories of sensitive data. Most sensitive data types are monitored.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of sensitive data assets. Data ownership has been defined for sensitive data elements.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their cloud infrastructure and monitor the remediation of the risks and revise the risk assessment results accordingly.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.

them. Residual risks are accepted by the risk owners.		
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The extent of the competency and integrity review (screening) of all internal and external employees shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks. The competency and integrity of internal and external employees of the applicant shall be reviewed before commencement of employment in a position with a higher risk classification.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant’s code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant	Confidentiality / Integrity / Availability / Privacy / Accountability	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to customer data, the production environment, or any component thereof.

used to provide the service in the production environment.		
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties. The applicant shall update their security awareness and training program at least annually. The applicant shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group. The applicant shall measure and evaluate the learning outcomes achieved through the awareness and training programme.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall monitor the effectiveness of the policies/ procedures that change/ revoke accounts and logical access rights when the employment of an internal or external employee is terminated or changed. A checklist for the return/ change of assets should be followed by HR or the IT departments when the employment of an internal or external employee is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the applicant for the protection of confidential information and operational details. The agreements shall be accepted by external service providers and suppliers when the contract is agreed. The agreements shall be accepted by internal employees of the applicant before authorisation to access data of customers is granted.
Asset Management		

The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	An asset inventory or asset Register shall be maintained and periodically updated by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle. The information recorded with assets shall include the measures taken to manage the risks associated to the asset and the data it contains throughout its life cycle.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The policies and procedures for acceptable use and safe handling of assets shall address at least the all aspects of the asset lifecycle as applicable to the asset.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the service in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The procedure shall ensure that the risks arising from the commissioning are identified, analysed and mitigated. The procedure 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.
The applicant's internal and external employees are probably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant 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. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to customer data, the production environment, or any component thereof.
Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. When applicable, the applicant shall label all assets according to their classification in the asset classification schema.

information it processes, stores, or transmits.		
Physical Security		
The buildings and premises related to the cloud service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises. *	Confidentiality / Integrity / Availability	The security requirements shall be based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The applicant shall define and communicate a set of security requirements for each security area.
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process cloud customer data. The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay. The access control policy shall include logging of all accesses to non-public areas that enables the applicant to check whether only defined personnel have entered these zones.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity / Availability	The policies and procedures shall include a clear screen policy and a clear desk policy for documents and removable media.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. In case the applicant is a cloud provider, policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place.

The premises from which the cloud service operated, and in particular its data centres, are protected against external and environmental threats. *	Integrity / Availability	The security requirements for datacentres shall be based on criteria which comply with established rules of technology. The applicant shall provide the cloud service from at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience. The applicant shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks. *	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload. The applicant 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.
The capacities of critical resources such as personnel and IT resources are monitored. *	Integrity / Availability	The applicant 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.
Policies are defined that ensure the protection against malware of IT equipment related to the infrastructure.	Confidentiality / Integrity / Availability	The applicant 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.
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	Signature-based and behaviour-based malware protection tools shall be updated at least daily.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers or Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted; and iii) Access to the backed-up data and the execution of restores is performed only by authorised persons.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall provide evidence on the operational effectiveness of monitoring their data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The restore tests shall assess if the specifications for the RTO and RPO agreed are met. Any deviation from the specification during the restore test shall be reported to the applicant's responsible person for assessment and remediation.

Policies are defined to govern logging and monitoring events on system components under the applicant’s responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; and v) Time synchronisation of system components.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) 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; ii) Anonymisation of the data whenever used in a context that goes beyond a single customer; iii) Period of storage reasonably related to the purposes of the collection; iv) Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and v) Provision of the derived data to users according to contractual agreements; and vi) Automated event monitoring
The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation. Log data shall be deleted when it is no longer required for the purpose for which they were collected. 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. The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection.
Log data can be unambiguously attributed to a CSC. *	Integrity / Privacy / Accountability	The applicant shall make available interfaces to conduct forensic analysis of infrastructure components and their network communication.

Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The applicant shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant 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.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least "critical" and "high" classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Regular identification of vulnerabilities; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall perform the vulnerability scanning on all system cloud components test at least once a month. The applicant 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 applicant, as identified in a risk analysis. The applicant shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall harden all the system components under their cloud infrastructure, according to accepted industry standards. The hardening requirements for each system component shall be documented.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the effectiveness of access request policies and procedures for at least: i) Normal access requests; ii) Privileged access requests; iii) emergency access requests; and iv) external employees' access request
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts or two-moth inactivity. The limits on authentication attempts used in mechanism for user accounts under the responsibility of the applicant shall be based on the risks on the accounts, associated access rights and authentication mechanisms The applicant 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.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The review defined shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. The applicant handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. The applicant shall perform periodic access reviews on applications of medium/ high criticality rating on a bi-annual basis.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks. 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. The applicant shall require strong authentication for accessing the administration interfaces used by the applicant.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to all environments of the applicant shall be authenticated, including non-production environments. Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security The applicant shall offer strong authentication methods to the customers for use with the accounts under their responsibility.

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	When creating credentials, compliance with specifications is enforced automatically as far as technically possible. The credential associated to a personal account should be changed on bi-monthly basis and when the credential is changed or renewed, the person associated to that account shall be notified. 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.
The assets in and around the cloud service are managed in a way that ensure that access restrictions are enforced between different categories of assets *	Confidentiality / Integrity / Privacy / Accountability	The applicant 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. The applicant shall timely inform a CSC whenever internal or external employees of the applicant 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: i) Cause, time, duration, type and scope of the access; and ii) Enough details to enable subject matters experts of the CSC to assess the risks of the access.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) Strong cryptography and security protocols are used (e.g., TLS, IPsec, SSH, etc.) to safeguard confidential information during transmission over open, public networks.
The applicant has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage *	Confidentiality / Privacy	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. 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.

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	The applicant shall follow the following measures with respect to key management: i) Generation of keys for different cryptographic systems and applications; ii) Issuing and obtaining public-key certificates; iii) Provisioning and activation of the keys; iv) Secure storage of keys including description of how authorised users get access; v) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; vi) Handling of compromised keys; and vii) Withdrawal and deletion of keys.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant 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.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements within its network, including at least: i) when the security zones are to be separated and when the infrastructure is to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; and iii) how the data traffic for administration and monitoring are segregated from each other at the network level.
The communication flows within the cloud, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant shall distinguish between trusted and untrusted networks, based on a risk assessment. The applicant shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable). The applicant 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. The applicant 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.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows. The system access authorisation for cross-network access shall be based on a security assessment according to the requirements of the cloud infrastructure or customers.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks. *	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by physically separated networks or by strongly encrypted VLANs.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The logical structure of the applicant's network 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.
Portability and Interoperability		
Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems *	Confidentiality / Availability	The cloud service shall be accessible by cloud services from other applicants or cloud customers. Communication on these interfaces shall use standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks shall be encrypted.

Contractual agreements define adequate information with regard to the migration of data following the termination of the contractual relationship. *	Confidentiality / Availability / Privacy	The applicant shall include in cloud service contractual agreements aspects concerning the termination of the contractual relationship: i) Type, scope and format of the data the applicant provides to the CSC; ii) Delivery methods of the data to the cloud customer; iii) Definition of the timeframe, within which the applicant makes the data available to the CSC; iv) Definition of the point in time as of which the applicant makes the data inaccessible to the CSC and deletes these; and v) The CSC's responsibilities and obligations to cooperate for the provision of the data.
Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems. *	Confidentiality / Privacy	The cloud customer's data deletion procedures shall prevent recovery by forensic means. The applicant shall track the deletion of the customer’s data, including metadata and data to read in the data backups, in a way allowing the cloud customer to track the deletion of its data.
Change and Configuration Management		
Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the documentation of changes in the system, operational and user documentation.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall define the testing scope prior to deployment. The applicant shall include safeguards that guarantee the confidentiality of the data during the whole process. The applicant 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.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall provide sufficient evidence on the obtained approvals that were gathered prior to deployment.

Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall define roles and rights for the authorised personnel or system components who are allowed to make changes to the cloud service in the production environment and also utilise version controls. 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.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall maintain a list of all third-party and open source software. In the case that the applicant provide cloud services, the list of dependencies of all third-parties and open source software shall be made available to customers upon request.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the cloud infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall ensure that production environments are physically or logically separated from development, test or pre-production environments. Data contained in the production environments shall not be used without data masking in development, test or pre-production environments in order not to compromise their confidentiality.

Appropriate measures are taken to identify vulnerabilities introduced in the cloud service during the development process. *	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the security safeguards that include but are not limited to the following aspects: i) Static Application Security Testing; ii) Dynamic Application Security Testing; iii) Code reviews by subject matter experts; and iv) Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of contractual agreement regarding the development of the cloud infrastructure or components thereof by a third party serving the following aspects: i) Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; ii) Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and iii) Sufficient verifications are carried out to rule out the existence of known vulnerabilities.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the following aspects related to third party risk management: i) Requirements for the assessment of risks resulting from the procurement of third-party services; ii) Requirements for the classification of third parties based on the risk assessment by the applicant; iii) Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; iv) Information security awareness and training requirements for staff; v) Applicable legal and regulatory requirements; vi) Requirements for dealing with vulnerabilities, security incidents, and malfunctions; vii) Specifications for the contractual agreement of these requirements; viii) Specifications for the monitoring of these requirements; and ix) 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, in case the applicant is a cloud provider,
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties. The applicant 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. The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.

A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; and viii) Beginning of service usage.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall inform the customers affected by security incidents in a timely and appropriate manner. The applicant shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall maintain a catalogue (Incident Classification Matrix) that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents. 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. The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant 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. The applicant shall inform its customers about the actions taken, according to the contractual agreements. The applicant shall define, make public and implement a single point of contact to report security events and vulnerabilities
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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 The applicant shall only contract supporting external bodies that are qualified incident response service providers or government agencies.

Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The documents and evidence shall be archived in a way that could be used as evidence in court. When the applicant requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the applicant shall contract a qualified incident response service provider only.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business continuity and disaster recovery and contigency 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.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed on a periodic basis and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; and viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); The business impact analysis resulting from these policies and procedures shall be reviewed at least once a year, or after significant organisational or environment related changes.

A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be periodically performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) 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); vi) Methods for putting the plans into effect; and The business continuity plan shall be reviewed at least once a year, or after significant organisational or environment-related changes.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document and implement procedures and measure its effectiveness for complying to these contractual requirements.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference of the infrastructure.	Privacy	The applicant 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.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked. The applicant shall inform customers for potential deviations and identified vulnerabilities.
Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow any customers to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.

Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall provide evidence on the followed policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall ensure that the Privacy policy is signed by all new internal and external employees upon onboarding. The applicant shall provide evidence for all controls in place that are applicable to the regulatory Data Protection requirements.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; and iii) secure disposal of personal data according to the regulatory Data Protection requirements.
User Documentation		
Provide information to assist the customer in the secure configuration, installation and use of the cloud service. *	Confidentiality / Integrity / Availability / Privacy	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: i) Instructions for secure configuration; ii) Information sources on known vulnerabilities and update mechanisms; iii) Error handling and logging mechanisms; iv) Authentication mechanisms; v) Roles and rights concept including combinations that result in an elevated risk; vi) Services and functions for administration of the cloud service by privileged users, and vii) Complementary Customer Controls (CCCs). The applicant shall describe in the user documentation all risks shared with the customer

Provide information to assist the customer in the secure configuration, installation and use of the cloud service *	Confidentiality / Integrity / Availability	The online register of vulnerabilities shall also include known vulnerabilities that affect assets provided by the applicant that the customers have to install, provide or operate themselves under the customers responsibility. The presentation of the vulnerabilities shall follow an industry-accepted scoring system for the description of vulnerabilities. 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.
Provide transparent information about the location of the data and of its processing	Confidentiality / Integrity / Privacy	The applicant shall provide information about i) The locations from administration and supervision may be carried out on the cloud infrastructure; ii) The locations to which any cloud customer data, meta-data or derived data may be transferred, processed or stored.
Provide a rationale for the assurance level target by the cloud service. *	Confidentiality / Integrity	The applicant 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 If the applicant claims compliance to security profiles for its cloud service, the justification shall cover the security profiles.
Provide the information required by customers that want to use the applicant as subservice organization for the cloud infrastructure. *	Privacy	If the applicant 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 applicant as subservice organization. The applicant shall make the documentation available to cloud customers upon request.
Dealing with Investigation Requests from Government Agencies		
Cloud customers are kept informed of ongoing investigations if legally permitted. *	Privacy / Accountability	The applicant shall subject investigation requests from government agencies to a legal assessment by subject matter experts. The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken. The applicant shall inform the affected CSC(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.
Investigators only have access to the data required for their investigation after validation of the legality of their request. *	Privacy / Accountability	When no clear limitation of the data is possible, the applicant shall anonymise or pseudonymise. the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.
Product Safety and Security		

Cloud customers have access to sufficient information about the cloud service through error handling and logging mechanisms *	Integrity / Accountability	The information provided shall be detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: i) Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); ii) Malfunctions during processing of automatic or manual actions; and iii) Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. The logged information shall be protected from unauthorised access and modification and can be deleted by the CSC. When the CSC is responsible for the activation or type and scope of logging, the applicant shall provide appropriate logging capabilities.
A suitable session management is used to protect confidentiality, availability, integrity and authenticity during interactions with the cloud service. *	Confidentiality / Integrity / Availability	A suitable session management system shall be used that at least corresponds to the state-of-the-art and is protected against known attacks
Software-defined networking is only used if the cloud user data is protected by appropriate measures. *	Confidentiality / Integrity / Availability	The applicant shall ensure the confidentiality of the cloud user data by suitable procedures when offering functions for software-defined networking (SDN). The applicant shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features.
Services for providing and managing virtual machines and containers to customers include appropriate protection measures. *	Confidentiality / Integrity / Availability	The applicant shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: i) The CSC can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this CSC can only launch the images or containers released according to these restrictions; ii) In addition, these images provided by the applicant are hardened according to generally accepted industry standards.

5.3 TAAF Level 3

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes with respect to its infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall have obtained a valid ISO/IEC 27001 certification.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the cloud infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions. The applicant shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain a list with the competent authorities in terms of information security and relevant technical groups on an bi-annual basis to stay informed about current threats and vulnerabilities that are specific to their sector.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the cloud service, regardless of the nature of the project. The applicant shall include the review and signoff from the Information Security Officer, prior to the initiation of a new project.

Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least annually. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. The applicant's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of the cloud infrastructure. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees. Policies and procedures updates are communicated internally through different notification channels.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions to a security policy or procedure shall be approved by the top management or the Information Security Officer or at least a body who approved the security policy or procedure. The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.
Information Management		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over applicable controls that correspond to the handling policies and procedures, which should include specific for all data life cycle phases according to the data classification policies and procedures: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall use data labelling tool, which shall be consistently performed across most BUs for sensitive, unstructured data in accordance with data classification policies. Approved storage locations have been identified and configured for automatic data labelling as per the data classification policies and procedures, whilst data tagging is not performed on legacy data.

Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place. The applicant shall enforce a CASB solution that will allow expand the discovery capabilities of sensitive data on sanctioned third party cloud apps.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to storage devices are logged and prevented or owned based on the content of the information being transferred. A periodic review of the rules is conducted to update the rules to monitor and prevent new data types.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of information assets is maintained and assets are classified by the type of data contained and the relative risk. The inventory management is automated via the use of a centralized dashboard of a discovery tool.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels. The Risk Management Register should be updated at least on an annual basis.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their cloud infrastructure and monitor the remediation of the risks and revise the risk assessment results via an automated dashboard or risk compliance solution.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans. The applicant shall monitor the effectiveness of the risk treatment activities via an automated dashboard or risk compliance solution.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties. The applicant should provide evidence of employees' Information Security training on unacceptable behaviour or insider threat cases.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity review (screening) of internal and external employees of the applicant shall be conducted for the employees in all positions.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant used to provide the service in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The verification of the acknowledgement of information security policies and procedures shall be automatically monitored by the applicant. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.

The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the security awareness and training program. The applicant shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme. The applicant shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the logical access rights of users and assets of internal or external employees.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall periodically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers. More specifically, the requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly. The applicant shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall automatically monitor the asset inventory via the provisioning of an inventory tool to ensure that all entries on the inventory are up-to-date.

Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use. Exception forms should be used for requesting the use of removable media. Specific training and awareness modules with mandatory attendance should be in place for all internal and external employees with respect to safe handling of assets.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned, which is used to provide the service in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The approval of the commissioning and decommissioning of hardware shall be automatically monitored.
The applicant's internal and external employees are probably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of the service. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant 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. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. The requirements for sufficient asset protection shall be determined by the individuals or groups responsible for the assets (asset owners) and the Information Security Officer.
Physical Security		

The buildings and premises related to the cloud service provided are divided into zones by security perimeters, depending on the level on information security risk associated to the activities performed and assets stored in these buildings and premises. *	Confidentiality / Integrity / Availability	The applicant shall define at least an additional private area that may host development activities and administration, supervision and operation workstations. The applicant shall ensure that no direct access exists between a public area and a sensitive area. The applicant shall ensure that all delivery, loading areas, and other points through which unauthorised persons can penetrate into the premises without being accompanied are part of the public area.
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users The logging of accesses shall be automatically monitored and reviewed on an annual basis.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity / Availability	The applicant shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area. The applicant shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. In case the applicant is a cloud provider, policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place. The applicant shall ensure that any back-up equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted or has been destroyed beforehand using a secure deletion mechanism.
The premises from which the cloud service operated, and in particular its data centres, are protected against external and environmental threats. *	Integrity / Availability	The security requirements for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime. The security requirements for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually.

Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks. *	Availability	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning.
The capacities of critical resources such as personnel and IT resources are monitored. *	Integrity / Availability	The applicant shall make available to the cloud customer the relevant information regarding capacity and availability on a self-service portal. The provisioning and de-provisioning of cloud services shall be automatically monitored.
Policies are defined that ensure the protection against malware of IT equipment related to the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces. The applicant shall update the anti-malware products at the highest frequency that the vendors actually offer.
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms. The applicant shall automatically monitor the antimalware full scans to track detected malware or irregularities on a daily basis.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) 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); ii) Data is backed up in encrypted, state-of-the-art form; iii) Access to the backed-up data and the execution of restores is performed only by authorised persons; and iv) Tests of recovery procedures.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall configure a portal for automatically monitoring their scheduled data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The applicant shall inform cloud customers or users, at their request, of the results of the recovery tests. Recovery tests shall be aligned with applicant’s business continuity management requirements.

Policies are defined to govern logging and monitoring events on system components under the applicant’s responsibility.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions to ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; v) Time synchronisation of system components; and vi) Compliance with legal and regulatory frameworks. The Applicant shall implement a centralized logging repository mechanism that is available 24/7 relevant to the cloud infrastructure.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments. The applicant shall automatically monitor that event detection is effective on the list of critical assets.
The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection. The applicant shall automatically monitor the aggregation and deletion of logging and monitoring data.
Log data can be unambiguously attributed to a CSC. *	Integrity / Privacy / Accountability	In the context of an investigation of an incident concerning a Cloud service customer, the applicant shall have the ability to provide to the customer the logs related to its cloud service.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The access to system components for logging and monitoring shall require strong authentication.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant shall design the system components for logging and monitoring in such a way that the overall functionality is not restricted if individual components fail.

Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Automated identification of vulnerabilities through a commercial tool; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	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 threat landscape. Some of the penetration tests performed each year shall be performed by external service providers. The applicant 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 systems. The applicant shall correlate the possible exploits of discovered vulnerabilities with previous incidents to identify if the vulnerability may have been exploited before its discovery.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall quarterly perform and review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness.
System components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the cloud components according to the appropriate hardening specifications.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the use of an automated ticketing tool that supports all user access requests.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall provide a sample of privileged users access rights to validate that no toxic combinations are present with reference to the Segregation of Duties Matrix. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall implement the process on all user accounts under its responsibility. The applicant shall automatically monitor the implemented automated mechanisms. The applicant shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall perform the user access rights via the use of an automated access review/ recertification tool.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	The applicant must revise every six (6) months the list of employees who are responsible for a technical account within its scope of responsibility. The applicant shall maintain an automated inventory of the user accounts under its responsibility that have privileged access rights.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to the production environment of the applicant shall require strong authentication. The access to all environments of the applicant containing customer data shall require strong authentication.

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant 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. Passwords of administrator accounts should be stored on logical key vaults.
The assets in and around the cloud service are managed in a way that ensure that access restrictions are enforced between different categories of assets *	Confidentiality / Integrity / Privacy / Accountability	The applicant shall separate the administration interfaces made available to CSCs from those made available to its internal and external employees, and in particular: i) The administration accounts under the responsibility of the applicant 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; ii) The administration interfaces made available to CSCs shall not allow for any connection from accounts under the responsibility of the applicant; and iii) The administration interfaces used by the applicant 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. The applicant 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.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) All data should implement strong encryption mechanisms for their transmission (in transit).
The applicant has established procedures and technical safeguards to prevent the disclosure of cloud customers' data during storage *	Confidentiality / Privacy	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.

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	For the secure storage of keys and other secrets used for the administration tasks, the applicant shall use a key vault and should rotate the keys on a quarterly basis.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network. The applicant shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements to connect within its network, including at least: i) when the security zones are to be separated and when the cloud customers are to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; iii) how the data traffic for administration and monitoring are segregated from each other at the network level; iv) what internal, cross-location communication is permitted; and v) what cross-network communication is allowed.
The communication flows within the cloud, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant 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. The applicant shall assess the risks of identified vulnerabilities in accordance with the risk management procedure and follow-up measures shall be defined and tracked. The applicant shall protect all SIEM logs to avoid tampering.

Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Each network perimeter shall be controlled by redundant and highly available security gateways. The applicant shall automatically monitor the control of the network perimeters.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks. *	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by usage of network addressing schemes or by strongly encrypted VLANs.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	In the case of an applicant providing Cloud Services, the logical structure of network documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions. The applicant shall perform a full review of the network topology documentation at least once a year.
Portability and Interoperability		
Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems *	Confidentiality / Availability	The applicant 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
Contractual agreements define adequate information with regard to the migration of data following the termination of the contractual relationship. *	Confidentiality / Availability / Privacy	The applicant shall identify, at least once a year, legal and regulatory requirements that may apply to these aspects and adjust the contractual agreements accordingly
Inbound and outbound interfaces to/from the cloud service are documented for access from other cloud services or IT systems. *	Confidentiality / Privacy	The cloud customer's data deletion procedures shall prevent recovery by forensic means The applicant shall track the deletion of the customer’s data, including metadata and data to read in the data backups, in a way allowing the cloud customer to track the deletion of its data. At the end of the contract, the applicant shall delete the technical data concerning the client.
Change and Configuration Management		

Policies and procedures are defined to control changes to information systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) 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; v) Requirements for the documentation of changes in the system, operational and user documentation; and vi) Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The tests performed any change before its deployment shall include tests on both a development environment, as well as testing environment. The applicant shall document and implement a procedure that ensures the integrity of the test data used in pre-production. The applicant shall perform penetration testing on components that are internet-facing. Before deploying changes on a system component, the applicant shall perform regression testing on other components of the cloud infrastructure that depend on that system component to verify the absence of undesirable effects. The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall automatically monitor the logs changes in the production environment to ensure that the principle of non-repudiation is maintained.
Development of Information Systems		

Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices via automated static or dynamic scanning tools.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall perform a risk assessment in accordance to Risk Management policies and procedures for every third party or open source software product.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the cloud infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The documentation of the tests of the security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test. The applicant shall consider the development and test environments when performing risk assessment. The applicant shall include development resources as part of the backup policy.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment.
Appropriate measures are taken to identify vulnerabilities introduced in the cloud service during the development process. *	Confidentiality / Integrity / Availability	Code reviews shall be regularly performed by qualified personnel or contractors. The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall 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. Internal or external employees of the applicant shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.

Procurement Management		
Responsibilities are assigned inside the organisation to ensure that third parties follow adequate security requirements.	Confidentiality / Integrity / Availability	The applicant 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. The reports shall include the complementary subservice organisation controls that are required, together with the controls of the applicant.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence over the organisation's third party management capabilities including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: i) Protection needs regarding the confidentiality, integrity and availability of information processed, stored, or transmitted by the third party; ii) Impact of a protection breach on the provision of the outsourcing service; iii)The applicant's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; vii) Security requirements; viii) Beginning of service usage; and ix) Proof of compliance with contractually agreed requirements.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall test the Incident Response Plan/ procedure at least on an annual basis.

A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall simulate the identification, analysis, and defence of security incidents and attacks on a quarterly basis through appropriate Table-top tests and exercises. The applicant shall review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness. The applicant shall monitor the processing of incident to verify the application of incident management policies and procedures.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow customers to actively approve the solution before automatically approving it after a certain period.
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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. 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The service provider shall establish an integrated team of forensic/ incident responder personnel specifically trained on evidence preservation and chain of custody management
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business business continuity and disaster recovery and contigency management and form a Business Continuity Management & Disaster Recoevry team, which is responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. The business continuity and disaster recovery and team shall ensure that sufficient resources are made available for an effective process.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed at least annually and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); ix) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and x) Estimation of the resources needed for resumption. The business impact analysis resulting from these policies and procedures shall be conducted and reviewed at regular intervals, at least once a year, or after significant organisational or environment related changes.

A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be at least annually performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) 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); vi) Methods for putting the plans into effect; vii) Continuous process improvement; and viii) Interfaces to Security Incident Management. The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall provide these procedures when requested by a customer. The applicant shall document and implement an active monitoring tool of the legal, regulatory and contractual requirements they need to follow.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference of the infrastructure.	Privacy	The applicant shall grant its customers contractually guaranteed information and define their audit rights.

Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions. The applicant shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate applicant's subject matter experts for immediate assessment and action.
Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow the customer to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. All commitments regarding locations of data processing and storage shall be enforced by the cloud service architecture.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall track the data request process via a ticketing system.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall document and implement an active monitoring tool of the regulatory Data Protection requirements they need to follow.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; iii) secure disposal of personal data according to the regulatory Data Protection requirements; iv) keeping a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.
User Documentation		

Provide information to assist the customer in the secure configuration, installation and use of the cloud service. *	Confidentiality / Integrity / Availability / Privacy	The applicant 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.
Provide information to assist the customer in the secure configuration, installation and use of the cloud service *	Confidentiality / Integrity / Availability	The applicant shall equip with automatic update mechanisms the assets it provides that must be installed, provided or operated by cloud customers within their area of responsibility.
Provide transparent information about the location of the data and of its processing	Confidentiality / Integrity / Privacy	The applicant 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.
Provide a rationale for the assurance level target by the cloud service. *	Confidentiality / Integrity	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.
Provide the information required by customers that want to use the applicant as subservice organization for the cloud infrastructure. *	Privacy	The applicant shall justify the contributions in a companion document
Dealing with Investigation Requests from Government Agencies		
Cloud customers are kept informed of ongoing investigations if legally permitted. *	Privacy / Accountability	The applicant shall subject investigation requests from government agencies to a legal assessment by subject matter experts. The legal assessment shall determine whether the government agency has an applicable and legally valid basis and what further steps need to be taken. The applicant shall inform the affected CSC(s) without undue delay, unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service
Investigators only have access to the data required for their investigation after validation of the legality of their request. *	Privacy / Accountability	The applicant shall automatically monitor the accesses performed by or on behalf of investigators to ensure that they correspond to the determined legal basis.
Product Safety and Security		

Cloud customers have access to sufficient information about the cloud service through error handling and logging mechanisms *	Integrity / Accountability	The applicant shall make the information available to CSCs via documented interfaces that are suitable for further processing this information as part of their Security Information and Event Management (SIEM).
A suitable session management is used to protect confidentiality, availability, integrity and authenticity during interactions with the cloud service. *	Confidentiality / Integrity / Availability	The session management system shall include mechanisms that invalidate a session after it has been detected as inactive. If inactivity is detected by time measurement, the time interval shall be configurable by the applicant or – if technically possible – by the CSC.
Software-defined networking is only used if the cloud user data is protected by appropriate measures. *	Confidentiality / Integrity / Availability	The applicant shall ensure that the configuration of networks matches network security policies regardless of the means used to create the configuration.
Services for providing and managing virtual machines and containers to customers include appropriate protection measures. *	Confidentiality / Integrity / Availability	The applicant shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: i)If the applicant provides images of virtual machines or containers to the CSC, the applicant appropriately inform the CSC of the changes made to the previous version. An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images.

6 Artificial Intelligence

Artificial Intelligence (AI) refers to that technology that leverages computers and machines to mimics the problem-solving, decision-making, and cognitive capabilities of the human mind.

6.1 TAAF Level 1

Objective	Applicable Type(s)	Description
Asset Management		
The applicant has established procedures for inventorying assets, including all AI assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall define an Asset Management Policy for maintaining an inventory of assets. The applicant shall periodically perform and update the asset mapping of AI assets based on the Asset Management Policy.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	Confidentiality / Integrity	The applicant shall document, communicate and implement policies and procedures for acceptable use and safe handling of assets.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The applicant shall document, communicate and implement a procedure for the commissioning of hardware in the production environment, based on applicable policies and procedures. This procedure mentioned shall include the complete and permanent deletion of the data or the proper destruction of the media.

The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant shall a procedure/ process that shall include steps to ensure that all assets under custody of an employee are returned upon termination of employment.
Assets are classified and, if possible, labelled. Classification and labelling of an AI asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	The applicant shall define an asset classification schema that reflects for each AI asset the protection needs of the information it processes, stores, or transmits.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for establishing the strategy and guidelines to ensure business continuity and disaster recovery and contigency management.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the AI model.	Availability	The applicant shall document, communicate and implement policies and procedures for performing a business impact assessment to determine the impact of any malfunction to the AI components.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The applicant shall document, communicate and implement a business continuity plan and disaster recovery plan to ensure continuity of the services, taking into account information security constraints and the results of the business impact assessment. The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used.

Change and Configuration Management		
Policies and procedures are defined to control changes to AI systems.	Confidentiality / Integrity / Availability / Accountability	The applicant shall document, implement, and communicate policies and procedures for change management of the AI systems.
Changes to the AI components are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the AI systems are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the AI systems are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are performed by authorized accounts.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures outlining technical safeguards and guidelines that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems.
The establishment of connections within the internal network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement specific security requirements aligned within its network security policy.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	The applicant shall define, document and implement policies and procedures outlining segregation mechanisms at network level to separate data traffic of different customers.

A map of the AI system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The applicant shall maintain up-to-date all documentation of the logical structure of the network.
Compliance		
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the AI systems' functionalities.	Privacy	The applicant shall document, communicate, make available and implement policies and procedures for planning and conducting internal audits.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control systems. The internal audit shall check the compliance with respect to their ISMS and regulatory frameworks. The applicant shall document specifically deviations that are nonconformities from their ISMS and regulatory frameworks including an assessment of their severity, and keep track of their remediation.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall define, communicate and implement policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall define, communicate and implement a Privacy policy outlining the entity’s objectives related to confidentiality and how confidential data are maintained. The Privacy Policy is reviewed and updated at least on an annual basis.
Appropriate technical controls are implemented to ensure compliance with the Ethical & Trustworthy AI Framework.		The applicant shall define, communicate and implement a Technical Blueprint defining the technical controls in place to ensure compliance with the Ethical & Trustworthy AI Framework.

Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The Applicant is shall define, communicate and implement policies and procedures to safeguard, protect, process and retain personal data.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall document, communicate, and implement policies and procedures that include technical and organizational safeguards for encryption and key management in which at least the following aspects are described: i) Usage of strong encryption procedures and secure network protocols ii) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys iii) Consideration of relevant legal and regulatory obligations and requirements
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The applicant shall document and implement procedures and technical safeguards to encrypt customers' data during storage.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	Procedures and technical safeguards for secure key management shall be defined and followed by the applicant.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of AI systems throughout their lifecycle.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures according to the technical and organisational measures for the secure development of the AI systems.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.
The development environment use logical or physical separation between production of AI environments.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure the separation of pre-production and production AI environments.

Appropriate measures are taken to identify vulnerabilities introduced in the AI service during the development process.	Confidentiality / Integrity / Availability	The applicant shall define appropriate safeguards or guidelines to check the AI service for vulnerabilities that may have been integrated into the AI service during the development process. The procedures for identifying vulnerabilities shall be integrated in the development process.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	When outsourcing development of the AI infrastructure or components thereof to a contractor, the applicant shall document, communicate and implement Third Party policies or procedures that address the security requirements of the outsourced software.
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the maintenance of its AI infrastructure in the production environment, and all positions with access to customer data and system components. The applicant shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: i) Verifying whether a violation has occurred; and ii) Consideration of the nature and severity of the violation and its impact. If disciplinary measures are defined in the policy, then the internal and external employees of the applicant shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity of all internal and external employees of the applicant with access to customer data or system components under the applicant's responsibility, or who will have access in the production environment shall be reviewed before commencement of employment in a position.

The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures. The applicant shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated as part of the AI infrastructure, even if anonymised and decontextualized.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a security awareness and training program that covers basic Information Security principles such as but not limited to: i) Handling system components used in the production environment in accordance with applicable policies and procedures; ii) Handling data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; iii) Information about the current threat situation; and iv) Correct behaviour in the event of security incidents. The applicant shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.
The applicant operates an awareness and training programa in place that the appropriate teams and individuals are adequately empowered trained and accountable for managing the risks of AI systems.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an awareness and training program that covers AI risk management principles and enables organization's personnel and partners to perform their duties and responsibilities consistent with related policies, procedures, and agreements.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define specific policies/ procedures that communicates to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed. The applicant shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized. AI applications shall comply with identity management, authentication, and access control policies.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make access policies and procedures for controlling access to information resources and based on the business and security requirements of the applicant, in which at least the following aspects are covered: i) Parameters to be considered for making access control decisions; ii) Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle; iii) Use of a role-based mechanism for the assignment of access rights; iv) Segregation of duties between managing, approving and assigning access rights v) Dedicated rules for users with privileged access; and vi) Requirements for the approval and documentation of the management of access rights. The applicant shall link the access control policy with the physical access control policy, to guarantee that the access to the premises where information is located is also controlled.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document policies for managing accounts in which at least the following aspects are described: i) Assignment of unique usernames; ii) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type. The applicant 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. The applicant 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. The applicant shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the AI service that comply with the role and rights concept and with the policies for managing accounts.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement general guidelines with respect to user access review/ recertification.

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The applicant shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: i) The selection of mechanisms suitable for every type of account; ii) The protection of credentials used by the authentication mechanism; and iii) The generation and distribution of credentials for new accounts.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: i) Non-reuse of credentials; ii) Recommendations for renewal of passwords; iii) Rules on the required strength of passwords, together with mechanisms to communicate and enforce the rules; and iv) Rules on storage of passwords; Passwords shall be only stored using cryptographically strong hash functions.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures according technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner, including all AI components.	Confidentiality / Integrity / Availability	The applicant 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement a procedure to archive all documents and evidence that provide details on security incidents The applicant 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.
Information Protection		

Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall document, communicate and implement information handling policies and procedures to protect the lifecycle of information in the organisation.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall document, communicate and implement information/ data classification policies and procedures to enforce appropriate safeguard and controls as per the confidentiality of data.
Controls are in place to ensure the quality of AI data.	Confidentiality / Integrity	The applicant shall document, communicate and implement policies and procedures to enforce appopriate safeguards to ensure AI data quality measures.
Information Security Policies		
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner. AI applications shall comply with information security policies and are integrated to security operations processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including: i) Objectives; ii) Scope; iii) Roles and responsibilities within the organization; v) Steps for the execution of the security strategy; vi) Applicable legal and regulatory requirements; The applicant shall communicate and make available the policies and procedures to all internal and external employees.

The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document a global Information Security policy covering at least the following aspects: i) the importance of information security, based on the requirements of AI infrastructure in relation to information security, as well as on the need to ensure the security of the information processed and stored by the applicant and the assets that support the services provided; ii) the security objectives and the desired security level, based on the business goals and tasks of the applicant; iii) the commitment of the applicant to implement the security measures required to achieve the established security objectives; iv) the most important aspects of the security strategy to achieve the security objectives set; and v) the organisational structure for information security in the ISMS application area. The applicant's top management shall approve and endorse its global information security policy. The applicant shall communicate and make available the global information security policy to internal and external employees and to AI service customers, in the case the applicant is a AI service provider.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall maintain a list of exceptions which are limited in time to the security policies and procedures, including associated controls. The list of exceptions shall be reviewed at least annually.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.

Policies are defined that ensure the protection against malware of IT equipment related to the AI service.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures to protect its systems and its customers from malware, covering at least the following aspects: i) Use of system-specific protection mechanisms ii) Operating protection programs on system components under the responsibility of the applicant that are used to provide the AI service in the production environment iii) Operation of protection programs for employees' terminal equipment
Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall deploy malware protection, if technically feasible, on all systems that support the AI infrastructure e in the production environment, according to policies and procedures.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for data backup and recovery.
Policies are defined to govern logging and monitoring events on AI components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the logging and monitoring of events on AI components.
Policies are defined to govern the management of data in the machine learning algorithms.	Integrity / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the use and management of data in used in machine learning algorithms.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	The log data generated allows an unambiguous identification of user accesses at the AI service customer level to support analysis in the event of an incident.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	Changes to the logging and monitoring configuration are made in accordance with applicable policies.
Vulnerabilities in the system components used in the AI components are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with respect to incident handling measures.
Documentation of AI core functionalities in Technical Blueprint	Confidentiality / Integrity / Availability	The applicant shall document the AI system's core functionality in a Technical Blueprint and maintains a register specifying how each aspect of functionality is defined, developed and implemented in the Blueprint.

AI system components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement general guidelines with respect to hardening AI infrastructure components.
Organisation of Information Security		
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall stay informed about current threats and vulnerabilities via a documented Threat Modelling process, which includes the identification of AI specific threats.
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a risk assessment methodology to be followed on its AI infrastructure. The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the AI service and are in the area of responsibility of the applicant: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the system components.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall have a documented an Information Security Policy/ process/ guidelines that outlines the need to include information security in the project management of all projects that may affect the service, regardless of the nature of the project.
Physical Security		

Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	scope of the AI ecosystem, as well as the evolving nature of AI systems and techniques.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall document, communicate, and implement policies and procedures concerning work in non-public areas.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning the Physical Security controls and safeguards in place. The applicant shall use encryption on removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media.
Data centres related to the AI service, are protected against external and environmental threats.	Integrity / Availability	The applicant shall document and communicate and implement policies and procedures outlining security requirements related to external and environmental threats, addressing the following risks in accordance with the applicable legal and contractual requirements: i) Faults in planning; ii) Unauthorised access; iii) Insufficient surveillance; iv) Insufficient air-conditioning; v) Fire and smoke; vi) Water; vii) Power failure; and viii) Air ventilation and filtration.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the AI infrastructure/ service. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the AI product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of AI services. Clear policies and procedures are in place to address AI risks arising from supply chain issues, including third-party software and data to ensure the trustworthiness of third-party data or AI systems. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the AI service.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall document risk management policies and procedures for the following aspects: i) Identification of risks associated with the loss of confidentiality, integrity, availability (CIA triad); authenticity of information within the scope of the ISMS and assigning risk owners ii) Analysis of the probability and impact of occurrence and determination of the level of risk; iii) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; iv) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and v) Documentation of the activities implemented to enable consistent, valid and comparable results.
Risk assessment-related policies and procedures are implemented on the AI service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall implement the policies and procedures covering AI risk assessment on the entire perimeter of the AI infrastructure. The applicant shall make the results of the risk assessment available to relevant stakeholders.

6.2 TAAF Level 2

Objective	Applicable Type(s)	Description
Asset Management		
The applicant has established procedures for inventorying assets, including all AI assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	An asset inventory or asset Register shall be maintained and periodically updated by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle. The information recorded with assets shall include the measures taken to manage the risks associated to the asset and the data it contains throughout its life cycle. All AI assets and components across the AI lifecycle stages are classified and the tasks they support are clearly defined.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	Confidentiality / Integrity	The policies and procedures for acceptable use and safe handling of assets shall address at least the all aspects of the asset lifecycle as applicable to the asset.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The procedure shall ensure that the risks arising from the commissioning are identified, analysed and mitigated. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof. The procedure 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.

The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant 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. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to customer data, the production environment, or any component thereof.
Assets are classified and, if possible, labelled. Classification and labelling of an AI asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. When applicable, the applicant shall label all assets according to their classification in the asset classification schema. The specific task that each AI system will support is defined (e.g., recommendation, classification, etc.).
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business continuity and disaster recovery and contigency 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.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the AI model.	Availability	The business impact assessment shall be performed on a periodic basis and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of allAI components and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; and viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); The business impact analysis resulting from these policies and procedures shall be reviewed at least once a year, or after significant organisational or environment related changes.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be periodically performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of AI infrastructure components and services and alignment with customers); vi) Methods for putting the plans into effect; and The business continuity plan shall be reviewed at least once a year, or after significant organisational or environment-related changes.
Change and Configuration Management		

Policies and procedures are defined to control changes to AI systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the documentation of changes in the system, operational and user documentation.
Changes to the AI components are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall define the testing scope prior to deployment. The applicant shall include safeguards that guarantee the confidentiality of the data during the whole process. The applicant 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.
Changes to the AI systems are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall provide sufficient evidence on the obtained approvals that were gathered prior to production deployment.
Changes to the AI systems are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall define roles and rights for the authorised personnel or system components who are allowed to make changes to the production environment and also utilise version controls. All changes to the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant 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.

The establishment of connections within the internal network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements within its network, including at least: i) when the security zones are to be separated and when the infrastructure is to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; and iii) how the data traffic for administration and monitoring are segregated from each other at the network level.
The communication flows within the AI systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant shall distinguish between trusted and untrusted networks, based on a risk assessment. The applicant shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable). The applicant 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. The applicant 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.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows. The system access authorisation for cross-network access shall be based on a security assessment according to the requirements of the AI infrastructure or customers.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	Secure network segregation and segmentation shall be ensured by physically separated networks or by strongly encrypted VLANs.
A map of the AI system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The logical structure of the applicant's network 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 customers' data are stored.
Compliance		

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the AI systems' functionalities.	Privacy	The applicant shall document and implement an audit programme that defines the scope and the frequency of the internal audits in accordance with the management of change, policies, and the results of the risk assessment.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked. The applicant shall inform customers for potential deviations and identified vulnerabilities.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall provide evidence on the followed policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall ensure that the Privacy policy is signed by all new internal and external employees upon onboarding. The applicant shall provide evidence for all controls in place that are applicable to the regulatory Data Protection requirements.
Appropriate technical controls are implemented to ensure compliance with the Ethical & Trustworthy AI Framework.		The applicant shall provide appropriate evidence of the technical controls implementation, in alignment with the Technical Blueprint, to ensure compliance with the Ethical & Trustworthy AI Framework.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; and iii) secure disposal of personal data according to the regulatory Data Protection requirements.
Cryptography and Key Management		

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) Strong cryptography and security protocols are used (e.g., TLS, IPsec, SSH, etc.) to safeguard confidential information during transmission over open, public networks.
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known only to the customer in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions. The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the customer.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	The applicant shall follow the following measures with respect to key management: i) Generation of keys for different cryptographic systems and applications; ii) Issuing and obtaining public-key certificates; iii) Provisioning and activation of the keys; iv) Secure storage of keys including description of how authorised users get access; v) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; vi) Handling of compromised keys; and vii) Withdrawal and deletion of keys.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of AI systems throughout their lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Best practices on AI Model Evaluation ii) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); iii) Security in software deployment (including continuous delivery); iv) Security in operation (reaction to identified faults and vulnerabilities); v) Best practices on algorithm robustness enhancement, algorithm fairness guarantee and algorithm interpretability improvement; and v) Secure coding standards and practices.

The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the AI infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
The development environment use logical or physical separation between production of AI environments.	Confidentiality / Integrity / Availability	The applicant shall ensure that production environments are physically or logically separated from development, test or pre-production AI environments. Data contained in the production environments shall not be used without data masking in development, test or pre-production environments in order not to compromise their confidentiality.
Appropriate measures are taken to identify vulnerabilities introduced in the AI service during the development process.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the security safeguards that include but are not limited to the following aspects: i) Static Application Security Testing; ii) Dynamic Application Security Testing; iii) Code reviews by subject matter experts; and iv) Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own AI service.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of contractual agreement regarding the development of the AI infrastructure or components thereof by a third party serving the following aspects: i) Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; ii) Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and iii) Sufficient verifications are carried out to rule out the existence of known vulnerabilities.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The extent of the competency and integrity review (screening) of all internal and external employees shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks. The competency and integrity of internal and external employees of the applicant shall be reviewed before commencement of employment in a position with a higher risk classification.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant’s code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position’s risk classification and technical duties. The applicant shall update their security awareness and training program at least annually. The applicant shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group. The applicant shall measure and evaluate the learning outcomes achieved through the awareness and training programme.

The applicant operates an awareness and training programa in place that the appropriate teams and individuals are adequately empowered trained and accountable for managing the risks of AI systems.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall update their AI risk management awareness and training program at least annually. The applicant shall ensure that all relevant employees complete the AI risk management awareness and training program on a regular basis. The applicant shall measure and evaluate the learning outcomes achieved through the AI risk management awareness and training programme.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall monitor the effectiveness of the policies/ procedures that change/ revoke accounts and logical access rights when the employment of an internal or external employee is terminated or changed. A checklist for the return/ change of assets should be followed by HR or the IT departments when the employment of an internal or external employee is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the applicant for the protection of confidential information and operational details. The agreements shall be accepted by external service providers and suppliers when the contract is agreed. The agreements shall be accepted by internal employees of the applicant before authorisation to access data of customers is granted.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized. AI applications shall comply with identity management, authentication, and access control policies.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the effectiveness of access request policies and procedures for at least: i) Normal access requests; ii) Privileged access requests; iii) emergency access requests; and iv) external employees' access request
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts or two-moth inactivity. The limits on authentication attempts used in mechanism for user accounts under the responsibility of the applicant shall be based on the risks on the accounts, associated access rights and authentication mechanisms The applicant 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.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The review defined shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. The applicant handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. The applicant shall perform periodic access reviews on applications of medium/ high criticality rating on a bi-annual basis.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks. 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. The applicant shall require strong authentication for accessing the administration interfaces used by the applicant.

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to all environments of the applicant shall be authenticated, including non-production environments. Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security The applicant shall offer strong authentication methods to the employees and AI service's customers for use with the accounts under their responsibility.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	When creating credentials, compliance with specifications is enforced automatically as far as technically possible. The credential associated to a personal account should be changed on bi-monthly basis and when the credential is changed or renewed, the person associated to that account shall be notified. 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.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall inform the customers affected by security incidents in a timely and appropriate manner. The applicant shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner, including all AI components.	Confidentiality / Integrity / Availability	The applicant shall maintain a catalogue (Incident Classification Matrix) that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents. 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. The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant 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. The applicant shall inform its customers about the actions taken, according to the contractual agreements. The applicant shall define, make public and implement a single point of contact to report security events and vulnerabilities
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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 The applicant shall only contract supporting external bodies that are qualified incident response service providers or government agencies.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The documents and evidence shall be archived in a way that could be used as evidence in court. When the applicant requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the applicant shall contract a qualified incident response service provider only.

Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over the applicable controls that correspond to the data handling policies and procedures, which should include controls for all data life cycle phases: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall classify all data according to the data classification policies and procedures on both structured and unstructured data.
Controls are in place to ensure the quality of AI data.	Confidentiality / Integrity	The applicant shall ensure the data will suit the model and limit the ingestion of malicious data via implementing the following controls: i) evaluation of the trust level of the sources to check its suitability in the context of the application ii) protection of their integrity along the whole data supply chain iii)verification their format and consistence.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to external storage devices are monitored and prevented for certain categories of sensitive data. Most sensitive data types are monitored.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of sensitive data assets. Data ownership has been defined for sensitive data elements.
Information Security Policies		

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner. AI applications shall comply with information security policies and are integrated to security operations processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions shall be subjected to the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload. The applicant shall meet the requirements included in contractual agreements with customers regarding the provision of the AI service in case of capacity bottlenecks or personnel and IT resources outages.
The capacities of critical resources such as personnel and IT resources are monitored.	Integrity / Availability	The applicant shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning for the IT resources.
Policies are defined that ensure the protection against malware of IT equipment related to the AI service.	Confidentiality / Integrity / Availability	The applicant 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.

Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	Signature-based and behaviour-based malware protection tools shall be updated at least daily.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the on premises operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted; and iii) Access to the backed-up data and the execution of restores is performed only by authorised persons.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall provide evidence on the operational effectiveness of monitoring their data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The restore tests shall assess if the specifications for the RTO and RPO agreed are met. Any deviation from the specification during the restore test shall be reported to the applicant's responsible person for assessment and remediation.
Policies are defined to govern logging and monitoring events on AI components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; and v) Time synchronisation of system components.
Policies are defined to govern the management of data in the machine learning algorithms.	Integrity / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Purpose for the collection and use of derived data beyond the operation of the AI service, including purposes related to the implementation of security controls; ii) Anonymisation of the data whenever used in a context that goes beyond a single customer; iii) Period of storage reasonably related to the purposes of the collection; iv) Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and v) Provision of the derived data to users according to contractual agreements; and vi) Automated event monitoring

The security of logging and monitoring of AI data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation. Log data shall be deleted when it is no longer required for the purpose for which they were collected. 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. The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	The applicant shall make available interfaces to conduct forensic analysis of AI components and their network communication.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The applicant shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility.
Vulnerabilities in the system components used in the AI components are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least "critical" and "high" classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Regular identification of vulnerabilities; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the AI service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall perform the vulnerability scanning on all system components test at least once a month. The applicant 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, as identified in a risk analysis. The applicant shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.

Documentation of AI core functionalities in Technical Blueprint	Confidentiality / Integrity / Availability	The applicant shall provide evidence of technical controls specific to the AI components and applications, based on the Technical Blueprint documentation.
AI system components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall harden all the system components under their AI infrastructure, according to accepted industry standards. The hardening requirements for each system component shall be documented.
Organisation of Information Security		
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain a list of applicable current threats, including AI specific threats. The applicant shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's ISMS shall be based in accordance to ISO/IEC 27001.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the applicant's AI infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the AI service, regardless of the nature of the project.

Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process customer data. The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay. The access control policy shall include logging of all accesses to non-public areas that enables the applicant to check whether only defined personnel have entered these zones.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The policies and procedures shall include a clear screen policy and a clear desk policy for documents and removable media.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place.
Data centres related to the AI service, are protected against external and environmental threats.	Integrity / Availability	The applicant shall provide at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience. The applicant shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the following aspects related to third party risk management: i) Requirements for the assessment of risks resulting from the procurement of third-party services; ii) Requirements for the classification of third parties based on the risk assessment by the applicant; iii) Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; iv) Information security awareness and training requirements for staff; v) Applicable legal and regulatory requirements; vi) Requirements for dealing with vulnerabilities, security incidents, and malfunctions; vii) Specifications for the contractual agreement of these requirements; viii) Specifications for the monitoring of these requirements.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the AI product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties. The applicant 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. The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; and viii) Beginning of service usage.

Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels.
Risk assessment-related policies and procedures are implemented on the AI service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their AI systems and monitor the remediation of the risks and revise the risk assessment results accordingly.
The applicant should regularly receive feedback from appropriate subject matter experts with respect to the performance, interended use and trustworthiness of the AI systems.	Integrity / Availability	The applicant shall perform at regular intervals external audits by subject matter experts to check whether the AI systems are performing consistently with their intended use and as expected in the specific deployment setting without deviations.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.

6.3 TAAF Level 3

Objective	Applicable Type(s)	Description
Asset Management		

The applicant has established procedures for inventorying assets, including all AI assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall automatically monitor the asset inventory via the provisioning of an inventory tool to ensure that all entries on the inventory are up-to-date. The applicant shall document a detailed AI asset taxonomy and include the functional description of specific stages in order to reflect AI components, but also assets that support the developments and deployment of AI systems.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media.	Confidentiality / Integrity	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use. Exception forms should be used for requesting the use of removable media. Specific training and awareness modules with mandatory attendance should be in place for all internal and external employees with respect to safe handling of assets.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The approval of the commissioning and decommissioning of hardware shall be automatically monitored. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment.	Confidentiality / Integrity	The applicant 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. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
Assets are classified and, if possible, labelled. Classification and labelling of an AI asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. The requirements for sufficient asset protection shall be determined by the individuals or groups responsible for the assets (asset owners) and the Information Security Officer. Detailed information is provided about the operational context in which the AI system will be deployed and how output will be utilized.

Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business business continuity and disaster recovery and contigency management and form a Business Continuity Management & Disaster Recoevry team, which is responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. The business continuity and disaster recovery and team shall ensure that sufficient resources are made available for an effective process.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the AI model.	Availability	The business impact assessment shall be performed at least annually and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of all AI components and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); ix) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and x) Estimation of the resources needed for resumption. The business impact analysis resulting from these policies and procedures shall be conducted and reviewed at regular intervals, at least once a year, or after significant organisational or environment related changes.

A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be at least annually performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of AI infrastructure components and services and alignment with customers); vi) Methods for putting the plans into effect; vii) Continuous process improvement; and viii) Interfaces to Security Incident Management. The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes
Change and Configuration Management		

Policies and procedures are defined to control changes to AI systems.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the proper information of AI service customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; v) Requirements for the documentation of changes in the system, operational and user documentation; and vi) Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.
Changes to the AI components are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The tests performed any change before its deployment shall include tests on both a development environment, as well as testing environment. The applicant shall document and implement a procedure that ensures the integrity of the test data used in pre-production. The applicant shall perform penetration testing on components that are internet-facing. Before deploying changes on a AI component, the applicant shall perform regression testing on other components of the AI infrastructure that depend on that system component to verify the absence of undesirable effects. The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the AI systems are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall monitor the execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the AI systems are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall automatically monitor the changes' logs in the production environment to ensure that the principle of non-repudiation is maintained.
Communication Security		

The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network. The applicant shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines.
The establishment of connections within the internal network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements to connect within its network, including at least: i) when the security zones are to be separated and when the customers are to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; iii) how the data traffic for administration and monitoring are segregated from each other at the network level; iv) what internal, cross-location communication is permitted; and v) what cross-network communication is allowed.
The communication flows within the AI systems, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant 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. The applicant shall assess the risks of identified vulnerabilities in accordance with the risk management procedure and follow-up measures shall be defined and tracked. The applicant shall protect all SIEM logs to avoid tampering.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Each network perimeter shall be controlled by redundant and highly available security gateways. The applicant shall automatically monitor the control of the network perimeters.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	Secure network segregation and segmentation shall be ensured by physically separated networks or by strongly encrypted VLANs.

A map of the AI system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	In the case of an applicant providing AI services, the logical structure of network documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions. The applicant shall perform a full review of the network topology documentation at least on an annual basis.
Compliance		
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the AI systems' functionalities.	Privacy	The applicant shall document and implement an audit programme that defines the scope and the frequency of the internal audits in accordance with the management of change, policies, and the results of the risk assessment. Subject matter experts shall assist in measuring and validating whether the system is performing consistently with their intended use and as expected in the specific deployment setting. Measurable performance improvements (e.g., participatory methods) based on consultations are identified.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions. The applicant shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate applicant's subject matter experts for immediate assessment and action.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall track the data request process via a ticketing system.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall document and implement an active monitoring tool, where appropriate, of the regulatory Data Protection requirements they need to follow.
Appropriate technical controls are implemented to ensure compliance with the Ethical & Trustworthy AI Framework.		The applicant shall provide appropriate evidence of the maintanance and ongoing monitoring of technical controls, in alignment with the Technical Blueprint, to ensure compliance with the Ethical & Trustworthy AI Framework.

Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; iii) secure disposal of personal data according to the regulatory Data Protection requirements; iv) keeping a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) All data should implement strong encryption mechanisms for their transmission (in transit).
The applicant has established procedures and technical safeguards to prevent the disclosure of customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known exclusively by the customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	For the secure storage of keys and other secrets used for the administration tasks, the applicant shall use designated key vaults and should rotate the keys on a quarterly basis.
Development of Information Systems		

Policies are defined to define technical and organisational measures for the development of AI systems throughout their lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Best practices on AI Model Evaluation ii) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); iii) Security in software deployment (including continuous delivery); iv) Security in operation (reaction to identified faults and vulnerabilities); v) Perform algorithm robustness enhancement, algorithm fairness guarantee and algorithm interpretability improvement; and vi) Secure coding standards and practices via automated static or dynamic scanning tools.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that ensures the management of the entire development cycle of the information system of the AI infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
The development environment use logical or physical separation between production of AI environments.	Confidentiality / Integrity / Availability	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for a production AI environment.
Appropriate measures are taken to identify vulnerabilities introduced in the AI service during the development process.	Confidentiality / Integrity / Availability	Code reviews shall be regularly performed by qualified personnel or contractors. The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall 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. Internal or external employees of the applicant shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties. The applicant should provide evidence of employees' Information Security training on unacceptable behaviour or insider threat cases.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity review (screening) of internal and external employees of the applicant shall be conducted for the employees in all positions.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The verification of the acknowledgement of information security policies and procedures shall be automatically monitored by the applicant. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to this.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the security awareness and training program. The applicant shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training program. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training program. The applicant shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks.

The applicant operates an awareness and training programa in place that the appropriate teams and individuals are adequately empowered trained and accountable for managing the risks of AI systems.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the AI risk management awareness and training program. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training program. The applicant shall verify the effectiveness of the AI risk management awareness and training program using practical exercises in awareness training that simulate actual AI risk management scenarios.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the logical access rights of users and assets of internal or external employees.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall periodically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers. More specifically, the requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly. The applicant shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized. AI applications shall comply with identity management, authentication, and access control policies.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the use of an automated ticketing tool that supports all user access requests.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall provide a sample of privileged users access rights to validate that no toxic combinations are present with reference to the Segregation of Duties Matrix. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall implement the process on all user accounts under its responsibility. The applicant shall automatically monitor the implemented automated mechanisms. The applicant shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall perform the user access rights via the use of an automated access review/ recertification tool.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	The applicant must revise every six (6) months the list of employees who are responsible for a technical account within its scope of responsibility. The applicant shall maintain an automated inventory of the user accounts under its responsibility that have privileged access rights.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to the production environment of the applicant shall require strong authentication. The access to all environments of the applicant containing data shall require strong authentication.

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant 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. Passwords of administrator accounts should be stored on logical key vaults.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall test the Incident Response Plan/ procedure at least on an annual basis.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner, including all AI components.	Confidentiality / Integrity / Availability	The applicant shall simulate the identification, analysis, and defence of security incidents and attacks on a quarterly basis through appropriate Table-top tests and exercises. The applicant shall review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness. The applicant shall monitor the processing of incident to verify the application of incident management policies and procedures.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow customers to actively approve the solution before automatically approving it after a certain period.
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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. 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The service provider shall establish an integrated team of forensic/ incident responder personnel specifically trained on evidence preservation and chain of custody management
Information Protection		

Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over applicable controls that correspond to the handling policies and procedures, which should include specific for all data life cycle phases according to the data classification policies and procedures: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall use data labelling tool, which shall be consistently performed across most BUs for sensitive, unstructured data in accordance with data classification policies. Approved storage locations have been identified and configured for automatic data labelling as per the data classification policies and procedures, whilst data tagging is not performed on legacy data.
Controls are in place to ensure the quality of AI data.	Confidentiality / Integrity	The applicant shall ensure the data will suit the model and limit the ingestion of malicious data via implementing the following controls: i) evaluation of the trust level of the sources to check its suitability in the context of the application ii) protection of their integrity along the whole data supply chain iii) verification their format and consistence.iv) their content is checked for anomalies, automatically or manually (e.g. selective human control); v) utilization of methods to clean the training dataset from suspicious samples; vi) in the case of labeled data, the issuer of the label is trusted.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place. The applicant shall enforce a solution that will allow expand the discovery capabilities of sensitive data on third party cloud apps.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to storage devices are logged and prevented or owned based on the content of the information being transferred. A periodic review of the rules is conducted to update the rules to monitor and prevent new data types.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of information assets is maintained and assets are classified by the type of data contained and the relative risk. The inventory management is automated via the use of a centralized dashboard of a discovery tool.
Information Security Policies		

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner. AI applications shall comply with information security policies and are integrated to security operations processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. The applicant's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of the AI infrastructure. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees. Policies and procedures updates are communicated internally through different notification channels.
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least annually. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions to a security policy or procedure shall be approved by the top management or the Information Security Officer or at least a body who approved the security policy or procedure. The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.
Operational Security		
The capacities of critical resources such as personnel and IT resources are planned in order to avoid possible capacity bottlenecks.	Availability	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning.
The capacities of critical resources such as personnel and IT resources are monitored.	Integrity / Availability	The applicant shall make available to the customer the relevant information regarding capacity and availability on a self-service portal. The provisioning and de-provisioning of the IT resources shall be automatically monitored.
Policies are defined that ensure the protection against malware of IT equipment related to the AI service.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces. The applicant shall update the anti-malware products at the highest frequency that the vendors actually offer.

Malware protection is deployed and maintained on systems that provide in the infrastructure.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms. The applicant shall automatically monitor the antimalware full scans to track detected malware or irregularities on a daily basis.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the on premises operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted, state-of-the-art form; iii) Access to the backed-up data and the execution of restores is performed only by authorised persons; and iv) Tests of recovery procedures.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall configure a portal for automatically monitoring their scheduled data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The applicant shall inform the AI service customers or users, at their request, of the results of the recovery tests. Recovery tests shall be aligned with applicant's business continuity management requirements.
Policies are defined to govern logging and monitoring events on AI components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions to ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; v) Time synchronisation of system components; and vi) Compliance with legal and regulatory frameworks. The Applicant shall implement a centralized logging repository mechanism hosted in Malta that is available 24/7 relevant to the AI infrastructure.
Policies are defined to govern the management of data in the machine learning algorithms.	Integrity / Privacy / Accountability	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments. The applicant shall automatically monitor that event detection is effective on the list of critical assets.

The security of logging and monitoring of AI data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection. The applicant shall automatically monitor the aggregation and deletion of logging and monitoring data.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	In the context of an investigation of an incident concerning a AI service customer, the applicant shall have the ability to provide to the customer the logs related to its service.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The access to system components for logging and monitoring shall require strong authentication.
Vulnerabilities in the system components used in the AI components are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Automated identification of vulnerabilities through a commercial tool; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the system components used to provide the AI service, in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	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 threat landscape. Some of the penetration tests performed each year shall be performed by external service providers. The applicant 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 on premises systems. The applicant shall correlate the possible exploits of discovered vulnerabilities with previous incidents to identify if the vulnerability may have been exploited before its discovery.

Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall quarterly perform and review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness.
Documentation of AI core functionalities in Technical Blueprint	Confidentiality / Integrity / Availability	The applicant shall deploy security protection components artificial intelligence applications, based on the AI Blueprint and help artificial intelligence applications more effectively resist data security attacks such as training data poisoning, model inversion attack, and membership inference attack.
AI system components are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the system components according to the appropriate hardening specifications.
Organisation of Information Security		
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain an a list of applicable threats based on ENISA's AI Threat Taxonomy which defines the current threat landscape. The applicant shall maintain a list of the competent authorities in terms of information security and relevant technical groups and update it on an bi-annual basis.
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall have obtained a valid ISO/IEC 27001 certification.

Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the AI infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions. The applicant shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the AI service, regardless of the nature of the project. The applicant shall include the review and signoff from the Information Security Officer, prior to the initiation of a new project.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users The logging of accesses shall be automatically monitored and reviewed on an annual basis.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area. The applicant shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area.

The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place. The applicant shall ensure that any back-up equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted or has been destroyed beforehand using a secure deletion mechanism.
Data centres related to the AI service, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime. The security requirements for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant 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. The reports shall include the complementary subservice organisation controls that are required, together with the controls of the applicant.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the AI product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence over the organisation's third party management capabilities including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: i) Protection needs regarding the confidentiality, integrity and availability of information processed, stored, or transmitted by the third party; ii) Impact of a protection breach on the provision of the outsourcing service; iii)The applicant's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible contigency plans. iv) Contingency processes are in place to address potential issues with third-party data or AI systems.

A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; vii) Security requirements; viii) Beginning of service usage; and ix) Proof of compliance with contractually agreed requirements.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels. The Risk Management Register should be updated at least on an annual basis.
Risk assessment-related policies and procedures are implemented on the AI service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their AI systems and monitor the remediation of the risks and revise the risk assessment results via an automated dashboard or risk compliance solution.
The applicant should regularly receive feedback from appropriate subject matter experts with respect to the performance, interended use and trustworthiness of the AI systems.	Integrity / Availability	External subject matter experts should provide measurable performance improvements (e.g., participatory methods) based on identified deviations. Identified AI algorithm or application related deviations should be defined, tracked. The applicant shall inform customers for potential deviations in terms of AI functionality, trustworthiness and intended use.

Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans. The applicant shall monitor the effectiveness of the risk treatment activities via an automated dashboard or risk compliance solution.

7 Internet of Things

The Internet of Things (IoT) refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

7.1 TAAF Level 1

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the IoT devices.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a risk assessment methodology to be followed. The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the IoT devices and are in the area of responsibility of the applicant: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the system components.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall stay informed about current threats and vulnerabilities via a documented Threat Modelling process.

Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall have a documented an Information Security Policy/ process/ guidelines that outlines the need to include information security in the project management of all projects that may affect the service, regardless of the nature of the project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document a global Information Security policy covering at least the following aspects: i) the importance of information security, based on the requirements of the IoT devices in relation to information security, as well as on the need to ensure the security of the information processed and stored by the applicant and the assets that support the services provided; ii) the security objectives and the desired security level, based on the business goals and tasks of the applicant; iii) the commitment of the applicant to implement the security measures required to achieve the established security objectives; iv) the most important aspects of the security strategy to achieve the security objectives set; and v) the organisational structure for information security in the ISMS application area. The applicant's top management shall approve and endorse its global information security policy. The applicant shall communicate and make available the global information security policy to internal and external employees.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including: i) Objectives; ii) Scope; iii) Roles and responsibilities within the organization; v) Steps for the execution of the security strategy; vi) Applicable legal and regulatory requirements; The applicant shall communicate and make available the policies and procedures to all internal and external employees.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall maintain a list of exceptions which are limited in time to the security policies and procedures, including associated controls. The list of exceptions shall be reviewed at least annually.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall document, communicate and implement information handling policies and procedures to protect the lifecycle of information in the organisation.

Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall document, communicate and implement information/ data classification polies and procedures to enforce appropriate safeguard and controls as per the confidentiality of data.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall document risk management policies and procedures for the following aspects: i) Identification of risks associated with the loss of confidentiality, integrity, availability (CIA triad); ii) authenticity of information within the scope of the ISMS and assigning risk owners iii) Analysis of the probability and impact of occurrence and determination of the level of risk; iv) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; v) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and vi) Documentation of the activities implemented to enable consistent, valid and comparable results.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall implement the policies and procedures covering risk assessment on all the IoT devices and resources. The applicant shall make the results of the risk assessment available to relevant stakeholders.
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the maintenance of IoT devices and resources in the production environment, and all positions with access to customer data and system components. The applicant shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: i) Verifying whether a violation has occurred; and ii) Consideration of the nature and severity of the violation and its impact. If disciplinary measures are defined in the policy, then the internal and external employees of the applicant shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.

The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity of all internal and external employees of the applicant with access to customer data or system components under the applicant's responsibility, or who will have access in the production environment shall be reviewed before commencement of employment in a position.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall ensure that all internal and external employees are required by their employment terms and conditions to comply with all applicable information security policies and procedures. The applicant shall ensure that the employment terms for all internal and external employees include a non-disclosure provision, which shall cover any information that has been obtained or generated, even if anonymised and decontextualized.
The applicant operates an IoT security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an IoT security awareness and training program that covers basic Information Security principles such as but not limited to: i) Handling system components used in the production environment in accordance with applicable policies and procedures; ii) Handling data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; iii) Information about the current threat situation; and iv) Correct behaviour in the event of security incidents. The applicant shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define specific policies/ procedures that communicates to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed. The applicant shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall ensure that non-disclosure or confidentiality agreements are agreed with internal employees, external service providers and suppliers.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall define an Asset Management Policy for maintaining an inventory of assets.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The applicant shall document, communicate and implement policies and procedures for acceptable use and safe handling of assets.

The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The applicant shall document, communicate and implement a procedure for the commissioning of hardware in the production environment, based on applicable policies and procedures. This procedure mentioned shall include the complete and permanent deletion of the data or the proper destruction of the media.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant shall a procedure/ process that shall include steps to ensure that all assets under custody of an employee are returned upon termination of employment.
IoT assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	The applicant shall define an asset classification schema for IoT devices that reflects for each asset the protection needs of the information it processes, stores, or transmits.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The applicant shall document, communicate and implement policies and procedures related to the physical access control to the security areas. The access control policy shall require at least one authentication factor for accessing any non-public area. The access control policy shall describe the physical access control derogations in case of emergency. The applicant shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters. The applicant shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner.

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall document, communicate, and implement policies and procedures concerning work in non-public areas.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning the Physical Security controls and safeguards in place. The applicant shall use encryption on removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The applicant shall document and communicate and implement policies and procedures outlining security requirements related to external and environmental threats, addressing the following risks in accordance with the applicable legal and contractual requirements: i) Faults in planning ii) Unauthorised access iii) Insufficient surveillance iv) Insufficient air-conditioning v) Fire and smoke vi) Water vii) Power failure viii) Air ventilation and filtration
Operational Security		
The capacities of critical resources such as personnel and IoT devices and resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.

Policies are defined that ensure the protection against malware of IoT devices and resources related.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures to protect its systems and its customers from malware, covering at least the following aspects: i) Use of system-specific protection mechanisms ii) Operating protection programs on system components under the responsibility of the applicant that are used to provide IoT service in the production environment iii) Operation of protection programs for employees' terminal equipment
Malware protection is deployed and maintained on IoT devices.	Confidentiality / Integrity / Availability	The applicant shall deploy malware protection, if technically feasible, on all IoT devices in the production environment, according to policies and procedures.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for data backup and recovery.
Policies are defined to govern logging and monitoring events on IoT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the logging and monitoring of events on IoT devices and resources.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the secure handling of derived data.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	The log data generated allows an unambiguous identification of user accesses at the customer level to support analysis in the event of an incident.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	Changes to the logging and monitoring configuration are made in accordance with applicable policies.
Vulnerabilities in the IoT devices and resources are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with respect to incident handling measures.
IoT devices and resources are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement general guidelines with respect to hardening on IoT devices and resources.

The configuration of the IoT devices' software can be changed, and such changes can be performed by authorized entities only.	Confidentiality / Integrity / Availability	The applicant shall define a standard, policy and a procedure for the unique identification of the entity's IoT device.
The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	Confidentiality / Integrity / Availability	The applicant shall have a patch management procedure defined.
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make access policies and procedures for controlling access to information resources and based on the business and security requirements of the applicant, in which at least the following aspects are covered: i) Parameters to be considered for making access control decisions ii) Granting and modifying access rights based on the "least-privilege" principle and on the "need-to-know" principle. iii) Use of a role-based mechanism for the assignment of access rights iv) Segregation of duties between managing, approving and assigning access rights v) Dedicated rules for users with privileged access vi) Requirements for the approval and documentation of the management of access rights The applicant shall link the access control policy with the physical access control policy, to guarantee that the access to the premises where information is located is also controlled.

Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document policies for managing accounts in which at least the following aspects are described: i) Assignment of unique usernames; ii) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type. The applicant 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. The applicant 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. The applicant shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the IoT device that comply with the role and rights concept and with the policies for managing accounts.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement general guidelines with respect to user access review/ recertification.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The applicant shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: i) The selection of mechanisms suitable for every type of account; ii) The protection of credentials used by the authentication mechanism; and iii) The generation and distribution of credentials for new accounts.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: i) Non-reuse of credentials; ii) Recommendations for renewal of passwords; iii) Rules on the required strength of passwords, together with mechanisms to communicate and enforce the rules; and iv) Rules on storage of passwords; Passwords shall be only stored using cryptographically strong hash functions.
A password policy with minimum security requirements is established for the IoT devices.	Confidentiality / Integrity / Privacy	The applicant shall have a documented password policy within the organization.
Cryptography and Key Management		

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall document, communicate, and implement policies and procedures that include technical and organizational safeguards for encryption and key management in which at least the following aspects are described: i) Usage of strong encryption procedures and secure network protocols ii) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys iii) Consideration of relevant legal and regulatory obligations and requirements
The applicant has established procedures and technical safeguards to prevent the disclosure of IoT devices' customers' data during storage.	Confidentiality / Privacy	The applicant shall document and implement procedures and technical safeguards to encrypt customers' data during storage.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	Procedures and technical safeguards for secure key management shall be defined and followed by the applicant.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures outlining technical safeguards and guidelines that are suitable to promptly detect and respond to network-based attacks and to ensure the protection of information and information processing systems.
The establishment of connections within the applicant’s network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement specific security requirements aligned within its network security policy.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	The applicant shall define, document and implement policies and procedures outlining segregation mechanisms at network level to separate data traffic of different customers.

A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The applicant shall maintain up-to-date all documentation of the logical structure of the network.
Change and Configuration Management		
Policies and procedures are defined to control changes to IoT devices.	Confidentiality / Integrity / Availability / Accountability	The applicant shall document, implement, and communicate policies and procedures for change management of the IoT devices.
Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are performed by authorized accounts.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures according to the technical and organisational measures for the secure development of the IoT device software. The policies and procedures for secure development shall consider information security from the earliest phases of design.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall document and implement policies for the use of third-party and open source software.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.

The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure the separation of pre-production and production environments.
Appropriate measures are taken to identify vulnerabilities introduced in the IoT device during the development process.	Confidentiality / Integrity / Availability	The applicant shall define appropriate safeguards or guidelines to check the IoT devices software for vulnerabilities that may have been integrated into IoT devices and resources during the development process. The procedures for identifying vulnerabilities shall be integrated in the development process.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	When outsourcing development of the on IoT devices software thereof to a contractor, the applicant shall document, communicate and implement Third Party policies or procedures that address the security requirements of the outsourced software.
A comprehensive test plan for the IoT devices software is established.	Confidentiality / Integrity / Privacy	The applicant shall should create a comprehensive testing plan to verify that the IoT product displays the expected features in both the software and hardware.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the IoT devices and resources. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring third parties whose products or services contribute to the provision of the IoT devices. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the IoT devices.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures according technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant 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

Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement a procedure to archive all documents and evidence that provide details on security incidents The applicant 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.
Threat modeling is performance for the whole IoT supply chain.	Confidentiality / Integrity	The applicant shall perform threat modeling for any critical IoT applications/devices in the suppy chain.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for establishing the strategy and guidelines to ensure business continuity and disaster recovery and contigency management.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The applicant shall document, communicate and implement policies and procedures for performing a business impact assessment to determine the impact of any malfunction to the IoT devices and resources.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The applicant shall document, communicate and implement a business continuity plan and disaster recovery plan to ensure continuity of the services, taking into account information security constraints and the results of the business impact assessment. The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the IoT devices.

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the IoT devices software.	Privacy	The applicant shall document, communicate, make available and implement policies and procedures for planning and conducting audits and addressing at least the following aspects: i) Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; ii) Activities that may result in malfunctions to breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and iii) Logging and monitoring of activities.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control systems. The internal audit shall check the compliance with respect to their ISMS and regulatory frameworks. The applicant shall document specifically deviations that are nonconformities from their ISMS and regulatory frameworks including an assessment of their severity, and keep track of their remediation.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall define, communicate and implement policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall define, communicate and implement a Privacy policy outlining the entity's objectives related to confidentiality and how confidential data are maintained. The Privacy Policy is reviewed and updated at least on an annual basis.
Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The applicant is shall define, communicate and implement policies and procedures to safeguard, protect, process and retain personal data.

7.2 TAAF Level 2

Objective	Applicable Type(s)	Description

Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's ISMS shall be based in accordance to ISO/IEC 27001.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the IoT devices.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the applicant's IoT devices and resources: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the IoT devices, regardless of the nature of the project.
Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.

Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions shall be subjected to the risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of the list of exceptions shall be reiterated at least annually, even if the list has not been updated.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over the applicable controls that correspond to the data handling policies and procedures, which should include controls for all data life cycle phases: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall classify all data according to the data classification policies and procedures on both structured and unstructured data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to external storage devices are monitored and prevented for certain categories of sensitive data. Most sensitive data types are monitored.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of sensitive data assets. Data ownership has been defined for sensitive data elements.

Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment all the IoT devices and resources and monitor the remediation of the risks and revise the risk assessment results accordingly.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.
Human Resources		
The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The extent of the competency and integrity review (screening) of all internal and external employees shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks. The competency and integrity of internal and external employees of the applicant shall be reviewed before commencement of employment in a position with a higher risk classification.

The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	All internal and external employees shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to customer data, the production environment, or any component thereof. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof.
The applicant operates an IoT security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an an IoT awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties. The applicant shall update their security awareness and training program at least annually. The applicant shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group. The applicant shall measure and evaluate the learning outcomes achieved through the awareness and training programme.
Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall monitor the effectiveness of the policies/ procedures that change/ revoke accounts and logical access rights when the employment of an internal or external employee is terminated or changed. A checklist for the return/ change of assets should be followed by HR or the IT departments when the employment of an internal or external employee is terminated or changed.

Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The non-disclosure or confidentiality agreements shall be based on the requirements identified by the applicant for the protection of confidential information and operational details. The agreements shall be accepted by external service providers and suppliers when the contract is agreed. The agreements shall be accepted by internal employees of the applicant before authorisation to access data of customers is granted.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	An asset inventory or asset Register shall be maintained and periodically updated by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle. The information recorded with assets shall include the measures taken to manage the risks associated to the asset and the data it contains throughout its life cycle.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	The policies and procedures for acceptable use and safe handling of assets shall address at least the all aspects of the asset lifecycle as applicable to the asset.
The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The procedure shall ensure that the risks arising from the commissioning are identified, analysed and mitigated. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to data, the production environment, or any component thereof. The procedure 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.

The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant 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. The applicant shall periodically give a presentation of the Acceptable Usage Policy to both internal and external employees prior to onboarding or granting them any access to customer data, the production environment, or any component thereof.
IoT assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on IoT asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. When applicable, the applicant shall label all assets according to their classification in the asset classification schema.
End-of-Life handling process is established for the Iot devices.	Confidentiality / Integrity / Privacy	The appplicant shall have a End-of-Life policy which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process customer data. The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay. The access control policy shall include logging of all accesses to non-public areas that enables the applicant to check whether only defined personnel have entered these zones.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The policies and procedures shall include a clear screen policy and a clear desk policy for documents and removable media.

The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall be based on criteria which comply with established rules of technology. The applicant shall provide at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience. The applicant shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises.
Operational Security		
The capacities of critical resources such as personnel and IoT devices and resources are planned in order to avoid possible capacity bottlenecks.	Availability	The applicant shall document and implement procedures to plan for capacities and resources, which shall include forecasting future capacity requirements in order to identify usage trends and manage system overload. The applicant shall meet the requirements included in contractual agreements with customers regarding the provision of IoT related resources in case of capacity bottlenecks.
The capacities of critical resources such as personnel and IoT devices and resources are monitored.	Integrity / Availability	The applicant shall define and implement technical and organizational safeguards for the monitoring of provisioning and de-provisioning for the IoT resources.
Policies are defined that ensure the protection against malware of IoT devices and resources related.	Confidentiality / Integrity / Availability	The applicant 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.
Malware protection is deployed and maintained on IoT devices.	Confidentiality / Integrity / Availability	Signature-based and behaviour-based malware protection tools shall be updated at least daily.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted; and iii) Access to the backed-up data and the execution of restores is performed only by authorised persons.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall provide evidence on the operational effectiveness of monitoring their data backups.

The proper restoration of data backups is regularly tested.	Integrity / Availability	The restore tests shall assess if the specifications for the RTO and RPO agreed are met. Any deviation from the specification during the restore test shall be reported to the applicant's responsible person for assessment and remediation.
Policies are defined to govern logging and monitoring events on IoT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; and v) Time synchronisation of system components.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Purpose for the collection and use of derived data beyond the operation of the IoT devices including purposes related to the implementation of security controls; ii) Anonymisation of the data whenever used in a context that goes beyond a single customer; iii) Period of storage reasonably related to the purposes of the collection; iv) Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and v) Provision of the derived data to users according to contractual agreements; and vi) Automated event monitoring
The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation. Log data shall be deleted when it is no longer required for the purpose for which they were collected. 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. The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	The applicant shall make available interfaces to conduct forensic analysis of infrastructure components and their network communication.

Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The applicant shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant 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.
Vulnerabilities in the IoT devices and resources are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least "critical" and "high" classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Regular identification of vulnerabilities; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of IoT devices and resources for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the IoT devices and resources in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall perform the vulnerability scanning on all system components test at least once a month. The applicant 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, as identified in a risk analysis. The applicant shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
IoT devices and resources are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall harden all the IoT devices, according to accepted industry standards. The hardening requirements for each IoT device type and resource shall be documented.
The configuration of the IoT devices' software can be changed, and such changes can be performed by authorized entities only.	Confidentiality / Integrity / Availability	The applicant shall ensure that the Identification Policy, uses a unique logical identifier that can be used to distinguish the device from all others.

The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	Confidentiality / Integrity / Availability	The applicant shall provide automatic update capabilities.
A security update policy for IoT devices with a constrained power source is in place.	Integrity / Availability	The applicant shall establish a security policy and balance the needs of maintaining the integrity and availability of the limited resources IoT devices.
A Security by Design approach has been estabilshed for the IoT devices.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document and develop a Security by Design program for IoT devices
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the effectiveness of access request policies and procedures for at least: i) Normal access requests; ii) Privileged access requests; iii) emergency access requests; and iv) external employees' access request
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts or two-moth inactivity. The limits on authentication attempts used in mechanism for user accounts under the responsibility of the applicant shall be based on the risks on the accounts, associated access rights and authentication mechanisms The applicant 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.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The review defined shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. The applicant handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. The applicant shall perform periodic access reviews on applications of medium/ high criticality rating on a bi-annual basis.

Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks. 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. The applicant shall require strong authentication for accessing the administration interfaces used by the applicant.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to all environments of the applicant shall be authenticated, including non-production environments. Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security The applicant shall offer strong authentication methods to the employees for use with the accounts under their responsibility.
Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	When creating credentials, compliance with specifications is enforced automatically as far as technically possible. The credential associated to a personal account should be changed on bi-monthly basis and when the credential is changed or renewed, the person associated to that account shall be notified. 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.
A password policy with minimum security requirements is established for the IoT devices.	Confidentiality / Integrity / Privacy	The applicant shall have enforced the password policy for the IoT devices.
The assets in and around the IoT devices and resources are managed in a way that ensure that access restrictions are enforced between different categories of assets	Confidentiality / Integrity / Privacy / Accountability	The applicant shall timely inform a customer whenever internal or external employees of the applicant access in a non-encrypted form to the customer's data processed, stored or transmitted in the IoT device without the prior consent of the customer, including at least: i) Cause, time, duration, type and scope of the access; and ii) Enough details to enable subject matters experts of the customer to assess the risks of the access.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) Strong cryptography and security protocols are used (e.g., TLS, IPsec, SSH, etc.) to safeguard confidential information during transmission over open, public networks.

The applicant has established procedures and technical safeguards to prevent the disclosure of IoT devices' customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known only to the customer in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions. The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be contractually agreed with the customer.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	The applicant shall follow the following measures with respect to key management: i) Generation of keys for different cryptographic systems and applications; ii) Issuing and obtaining public-key certificates; iii) Provisioning and activation of the keys; iv) Secure storage of keys including description of how authorised users get access; v) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; vi) Handling of compromised keys; and vii) Withdrawal and deletion of keys.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant 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.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements within its network, including at least: i) when the security zones are to be separated and when the infrastructure is to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; and iii) how the data traffic for administration and monitoring are segregated from each other at the network level.

The communication flows within the IoT devices and resources, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant shall distinguish between trusted and untrusted networks, based on a risk assessment. The applicant shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ, if applicable). The applicant 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. The applicant 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.
Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Security gateways shall only allow legitimate connections identified in a matrix of authorized flows. The system access authorisation for cross-network access shall be based on a security assessment according to the requirements of the IoT devices.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by physically separated networks or by strongly encrypted VLANs.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The logical structure of the applicant's network 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 customers' data are stored.
Change and Configuration Management		
Policies and procedures are defined to control changes to IoT devices.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the documentation of changes in the system, operational and user documentation.

Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall define the testing scope prior to deployment. The applicant shall include safeguards that guarantee the confidentiality of the data during the whole process. The applicant 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.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall provide sufficient evidence on the obtained approvals that were gathered prior to deployment.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall define roles and rights for the authorised personnel or system components who are allowed to make changes to the IoT device in the production environment and also utilise version controls. All changes to the IoT device in the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall maintain a list of all third-party and open source software.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the IoT device software. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	The applicant shall ensure that production environments are physically or logically separated from development, test or pre-production environments. Data contained in the production environments shall not be used without data masking in development, test or pre-production environments in order not to compromise their confidentiality.

Appropriate measures are taken to identify vulnerabilities introduced in the IoT device during the development process.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the security safeguards that include but are not limited to the following aspects: i) Static Application Security Testing; ii) Dynamic Application Security Testing; iii) Code reviews by subject matter experts; and iv) Obtaining information about confirmed vulnerabilities in software libraries provided by third parties.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of contractual agreement regarding the development of the IoT device software thereof by a third party serving the following aspects: i) Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; ii) Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and iii) Sufficient verifications are carried out to rule out the existence of known vulnerabilities.
A comprehensive test plan for the IoT devices software is established.	Confidentiality / Integrity / Privacy	The applicant shall perform acceptance testing independently from any previous testing that could have taken place in earlier stages in the supply chain.
IoT application protocols should be configured securely and update default configurations.	Confidentiality / Integrity	The applicant shall configure IoT application protocols (MQTT, AMQP, CoAP) securely.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the following aspects related to third party risk management: i) Requirements for the assessment of risks resulting from the procurement of third-party services; ii) Requirements for the classification of third parties based on the risk assessment by the applicant; iii) Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; iv) Information security awareness and training requirements for staff; v) Applicable legal and regulatory requirements; vi) Requirements for dealing with vulnerabilities, security incidents, and malfunctions; vii) Specifications for the contractual agreement of these requirements; viii) Specifications for the monitoring of these requirements.
Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties. The applicant 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. The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; and viii) Beginning of service usage.

Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall inform the customers affected by security incidents in a timely and appropriate manner. The applicant shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall maintain a catalogue (Incident Classification Matrix) that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents. 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. The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.
Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant 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. The applicant shall inform its customers about the actions taken, according to the contractual agreements. The applicant shall define, make public and implement a single point of contact to report security events and vulnerabilities
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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. The applicant shall only contract supporting external bodies that are qualified incident response service providers or government agencies.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The documents and evidence shall be archived in a way that could be used as evidence in court. When the applicant requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the applicant shall contract a qualified incident response service provider only.
Threat modeling is performance for the whole IoT supply chain.	Confidentiality / Integrity	The applicant shall have formal processes in place to perform threat modeling on critical applications in the suppy chain.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business continuity and disaster recovery and contigency 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.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed on a periodic basis and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; and viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); The business impact analysis resulting from these policies and procedures shall be reviewed at least once a year, or after significant organisational or environment related changes.
A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be periodically performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information; vi) Methods for putting the plans into effect; and The business continuity plan shall be reviewed at least once a year, or after significant organisational or environment-related changes.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall document and implement procedures and measure its effectiveness for complying to these contractual requirements.

Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the IoT devices software.	Privacy	The applicant 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.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked. The applicant shall inform customers for potential deviations and identified vulnerabilities.
Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow any customers to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall provide evidence on the followed policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall ensure that the Privacy policy is signed by all new internal and external employees upon onboarding. The applicant shall provide evidence for all controls in place that are applicable to the regulatory Data Protection requirements.
Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; and iii) secure disposal of personal data according to the regulatory Data Protection requirements.

7.3 TAAF Level 3

Objective	Applicable Type(s)	Description
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall have obtained a valid ISO/IEC 27001 certification.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of customer data processed, stored or transmitted in the IoT devices.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the IoT devices: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the system components; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions. The applicant shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain a list with the competent authorities in terms of information security and relevant technical groups on an bi-annual basis to stay informed about current threats and vulnerabilities that are specific to their sector.
Information security is considered in project management, regardless of the nature of the project.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the IoT devices, regardless of the nature of the project. The applicant shall include the review and signoff from the Information Security Officer, prior to the initiation of a new project.

Information Security Policies		
The top management of the applicant has adopted an information security policy and communicated it to internal and external employees as well as customers.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall review its global Information Security Policy at least annually. Appropriate governance practices for the security functions are defined and assign clear roles and responsibilities.
Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the applicant in an appropriate manner.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies. The applicant's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of IoT devices. After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees. Policies and procedures updates are communicated internally through different notification channels.
Exceptions to the policies and procedures for information security as well as respective controls are explicitly listed.	Confidentiality / Integrity / Availability / Privacy / Accountability	The exceptions to a security policy or procedure shall be approved by the top management or the Information Security Officer or at least a body who approved the security policy or procedure. The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all reviews and approvals are up-to-date.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over applicable controls that correspond to the handling policies and procedures, which should include specific for all data life cycle phases according to the data classification policies and procedures: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall use data labelling tool, which shall be consistently performed across most BUs for sensitive, unstructured data in accordance with data classification policies. Approved storage locations have been identified and configured for automatic data labelling as per the data classification policies and procedures, whilst data tagging is not performed on legacy data.

Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place. The applicant shall enforce a solution that will allow expand the discovery capabilities of sensitive data on sanctioned third party cloud apps.
DLP technologies should be configured monitor and restrict external file transfers.	Confidentiality / Privacy	File transfers to storage devices are logged and prevented or owned based on the content of the information being transferred. A periodic review of the rules is conducted to update the rules to monitor and prevent new data types.
The organisation shall manage the inventory of its sensitive data and data owners	Confidentiality / Privacy	The applicant maintains an inventory of information assets is maintained and assets are classified by the type of data contained and the relative risk. The inventory management is automated via the use of a centralized dashboard of a discovery tool.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of Information Assets, potential threats and vulnerabilities, mitigation approach and residual risk levels. The Risk Management Register should be updated at least on an annual basis.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on all the IoT devices and resources and monitor the remediation of the risks and revise the risk assessment results via an automated dashboard or risk compliance solution.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans. The applicant shall monitor the effectiveness of the risk treatment activities via an automated dashboard or risk compliance solution.
Human Resources		

The policies applicable to the management of internal and external employees include provisions that cover a risk classification of all information security-sensitive positions, a code of ethics, and a disciplinary procedure that applies to all of the employees involved in supplying the service who have breached the security policy.	Confidentiality / Integrity / Availability / Privacy / Accountability	All applicant's internal and external employees sign an Employment Agreement, a confidentiality and a non disclosure agreement to not disclose proprietary or confidential information, including client information, to unauthorized parties. The applicant should provide evidence of employees' Information Security training on unacceptable behaviour or insider threat cases.
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity review (screening) of internal and external employees of the applicant shall be conducted for the employees in all positions.
The applicant's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security, and to the applicant's code of ethics, before being granted access to any customer data or system components under the responsibility of the applicant in the production environment.	Confidentiality / Integrity / Availability / Privacy / Accountability	The verification of the acknowledgement of information security policies and procedures shall be automatically monitored by the applicant. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to this.
The applicant operates an IoT security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the an IoT security awareness and training program. The applicant shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme. The applicant shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the logical access rights of users and assets of internal or external employees.
Non-disclosure or confidentiality agreements are in place with internal employees, external service providers and suppliers of the applicant to protect the confidentiality of the information exchanged between them.	Confidentiality / Privacy	The applicant shall periodically monitor the confirmation of non-disclosure or confidentiality agreements by internal employees, external service providers and suppliers. More specifically, the requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually; if the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements shall be updated accordingly. The applicant shall inform its internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.
Asset Management		
The applicant has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall automatically monitor the asset inventory via the provisioning of an inventory tool to ensure that all entries on the inventory are up-to-date.
Policies and procedures for acceptable use and safe handling of assets are documented, communicated and provided, including in particular customer-owned assets and removable media	Confidentiality / Integrity	When removable media is used in the technical infrastructure or for IT administration tasks, this media shall be dedicated to a single use. Exception forms should be used for requesting the use of removable media. Specific training and awareness modules with mandatory attendance should be in place for all internal and external employees with respect to safe handling of assets.

The applicant has an approval procedure for the use of hardware to be commissioned or decommissioned in the production environment, depending on its intended use and based on the applicable policies and procedures.	Confidentiality / Integrity	The approval of the commissioning and decommissioning of hardware shall be automatically monitored. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
The applicant's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the applicant has determined in a risk assessment that loss or unauthorised access could compromise the information security of infrastructure. Any assets handed over are returned upon termination of employment	Confidentiality / Integrity	The applicant 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. Applicant should enforce both internal and external employees to sign an Acceptable Use Policy depicting their responsibility to adhere to security, integrity and availability of organisation's data or assets.
IoT assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.	Confidentiality / Integrity / Privacy	An asset register should be defined based on IoT asset classification schema, providing levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. The requirements for sufficient asset protection shall be determined by the individuals or groups responsible for the assets (asset owners) and the Information Security Officer.
End-of-Life handling process is established for the Iot devices.	Confidentiality / Integrity / Privacy	The applicant shall replace or decomission the End-of-Life IoT devices before the expiration of the End-of-Life period.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users The logging of accesses shall be automatically monitored and reviewed on an annual basis.

There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area. The applicant shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place. The applicant shall ensure that any back-up equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted or has been destroyed beforehand using a secure deletion mechanism.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime. The security requirements for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually.
Operational Security		
The capacities of critical resources such as personnel and IoT devices and resources are planned in order to avoid possible capacity bottlenecks.	Availability	The capacity projections shall be considered in accordance with the service level agreement for planning and preparing the provisioning.
The capacities of critical resources such as personnel and IoT devices and resources are monitored.	Integrity / Availability	The applicant shall make available to the customer the relevant information regarding capacity and availability on a self-service portal. The provisioning and de-provisioning of the IoT resources shall be automatically monitored.
Policies are defined that ensure the protection against malware of IoT devices and resources related.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces. The applicant shall update the anti-malware products at the highest frequency that the vendors actually offer.

Malware protection is deployed and maintained on IoT devices.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the IoT devices covered by the malware protection and the configuration of the corresponding mechanisms. The applicant shall automatically monitor the antimalware full scans to track detected malware or irregularities on a daily basis.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted, state-of-the-art form; iii) Access to the backed-up data and the execution of restores is performed only by authorised persons; and iv) Tests of recovery procedures.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall configure a portal for automatically monitoring their scheduled data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The applicant shall inform the on IoT device customers or users, at their request, of the results of the recovery tests. Recovery tests shall be aligned with applicant's business continuity management requirements.
Policies are defined to govern logging and monitoring events on IoT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions to ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; v) Time synchronisation of system components; and vi) Compliance with legal and regulatory frameworks. The Applicant shall implement a centralized logging repository mechanism hosted in Malta that is available 24/7 relevant to the IoT infrastructure.
Policies are defined to govern the management of derived data by the applicant.	Integrity / Privacy / Accountability	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments. The applicant shall automatically monitor that event detection is effective on the list of critical assets.

The security of logging and monitoring data are protected with measures adapted to their specific use.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: i) Access only to authorised users and systems; ii) Retention for the specified period; and iii) Deletion when further retention is no longer necessary for the purpose of collection. The applicant shall automatically monitor the aggregation and deletion of logging and monitoring data.
Log data can be unambiguously attributed to a customer.	Integrity / Privacy / Accountability	In the context of an investigation of an incident concerning a customer, the applicant shall have the ability to provide to the customer the logs related to its service.
Access to the logging and monitoring system components and to their configuration is strictly restricted.	Integrity / Accountability	The access to system components for logging and monitoring shall require strong authentication.
Systems for logging and monitoring are themselves monitored for availability.	Availability / Accountability	The applicant shall design the system components for logging and monitoring in such a way that the overall functionality is not restricted if individual components fail.
Vulnerabilities in the IoT devices and resources are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Automated identification of vulnerabilities through a commercial tool; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.

The applicant shall perform on a regular basis tests to detect publicly known vulnerabilities on the IoT devices and resources in accordance with policies for handling vulnerabilities.	Confidentiality / Integrity / Availability	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 threat landscape. Some of the penetration tests performed each year shall be performed by external service providers. The applicant 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 IoT devices and resoruces. The applicant shall correlate the possible exploits of discovered vulnerabilities with previous incidents to identify if the vulnerability may have been exploited before its discovery.
Incident handling measures are regularly evaluated and improved.	Confidentiality / Integrity / Availability	The applicant shall quarterly perform and review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness.
IoT devices and resources are hardened to reduce their attack surface and eliminate potential attack vectors.	Confidentiality / Integrity / Availability	The applicant shall automatically monitor the IoT devices and resources according to the appropriate hardening specifications.
The configuration of the IoT devices' software can be changed, and such changes can be performed by authorized entities only.	Confidentiality / Integrity / Availability	The applicant shall track the identification process via automated device management and monitoring.
The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	Confidentiality / Integrity / Availability	The applicant shall provide a rollback capability in case of an update failure.
A security update policy for IoT devices with a constrained power source is in place.	Integrity / Availability	The applicant shall enforce the security policy for all the limited resources IoT devices.
A Security by Design approach has been estabilshed for the IoT devices.	Confidentiality / Integrity / Availability / Privacy	The applicant shall review the Security By Design program once a year.
Identity, Authentication and Access Control Management		

Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the use of an automated ticketing tool that supports all user access requests.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall provide a sample of privileged users access rights to validate that no toxic combinations are present with reference to the Segregation of Duties Matrix. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall implement the process on all user accounts under its responsibility. The applicant shall automatically monitor the implemented automated mechanisms. The applicant shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall perform the user access rights via the use of an automated access review/ recertification tool.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	The applicant must revise every six (6) months the list of employees who are responsible for a technical account within its scope of responsibility. The applicant shall maintain an automated inventory of the user accounts under its responsibility that have privileged access rights.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to the production environment of the applicant shall require strong authentication. The access to all environments of the applicant containing data shall require strong authentication.

Throughout their lifecycle, authentication credentials are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant 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. Passwords of administrator accounts should be stored on logical key vaults.
A password policy with minimum security requirements is established for the IoT devices.	Confidentiality / Integrity / Privacy	The applicant shall review the enforcement password policy at least yearly.
The assets in and around the IoT devices and resources are managed in a way that ensure that access restrictions are enforced between different categories of assets	Confidentiality / Integrity / Privacy / Accountability	The applicant shall separate the administration interfaces made available to customers from those made available to its internal and external employees, and in particular: i) The administration accounts under the responsibility of the applicant shall be managed using tools and directories that are separate from those used for the management of user accounts under the responsibility of the customers; ii) The administration interfaces made available to customers shall not allow for any connection from accounts under the responsibility of the applicant; and iii) The administration interfaces used by the applicant shall not be accessible from the public network and as such shall not allow for any connection from accounts under the responsibility of the customer. The applicant shall require prior consent from a customer before any access in a non-encrypted formto the customer's data processed, stored or transmitted in the IoT device, providing meaningful information.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All servers and endpoints shall be encrypted at rest; and ii) All data should implement strong encryption mechanisms for their transmission (in transit).
The applicant has established procedures and technical safeguards to prevent the disclosure of IoT devices' customers' data during storage.	Confidentiality / Privacy	The private and secret keys used for encryption shall be known exclusively by the customer and without exceptions in accordance with applicable legal and regulatory obligations and requirements.

Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	For the secure storage of keys and other secrets used for the administration tasks, the applicant shall use a key vault and should rotate the keys on a quarterly basis.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall implement technical safeguards to ensure that no unknown (physical or virtual) devices join its (physical or virtual) network. The applicant shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines.
The establishment of connections within the applicant's network is subject to specific security requirements.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, make available and implement specific security requirements to connect within its network, including at least: i) when the security zones are to be separated and when the customers are to be logically or physically segregated; ii) what communication relationships and what network and application protocols are permitted in each case; iii) how the data traffic for administration and monitoring are segregated from each other at the network level; iv) what internal, cross-location communication is permitted; and v) what cross-network communication is allowed.
The communication flows within the IoT devices and resources, internal and external, are monitored according to the regulations to respond appropriately and timely to threats.	Confidentiality / Integrity / Availability / Accountability	The applicant 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. The applicant shall assess the risks of identified vulnerabilities in accordance with the risk management procedure and follow-up measures shall be defined and tracked. The applicant shall protect all SIEM logs to avoid tampering.

Cross-network access is restricted and only authorised based on specific security assessments.	Confidentiality / Integrity / Availability	Each network perimeter shall be controlled by redundant and highly available security gateways. The applicant shall automatically monitor the control of the network perimeters.
The confidentiality and integrity of customer data is protected by segregation measure when communicated over shared networks.	Confidentiality / Integrity	When implementing of infrastructure capabilities, the secure segregation shall be ensured by usage of network addressing schemes or by strongly encrypted VLANs.
A map of the information system is kept up and maintained, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of malfunctions.	Confidentiality / Integrity / Availability	The logical structure of network documentation shall include the equipment that provides security functions and the servers that host the data or provide sensitive functions. The applicant shall perform a full review of the network topology documentation at least once a year.
Change and Configuration Management		
Policies and procedures are defined to control changes to IoT devices.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the proper information of customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; v) Requirements for the documentation of changes in the system, operational and user documentation; and vi) Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.

Changes to the infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The tests performed any change before its deployment shall include tests on both a development environment, as well as testing environment. The applicant shall document and implement a procedure that ensures the integrity of the test data used in pre-production. The applicant shall perform penetration testing on components that are internet-facing. Before deploying changes on a IoT component, the applicant shall perform regression testing on other components to verify the absence of undesirable effects. The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall automatically monitor the logs changes in the production environment to ensure that the principle of non-repudiation is maintained.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of the infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices via automated static or dynamic scanning tools.
The applicant shall maintain a list of dependencies to hardware and software products used in the development of its infrastructure.	Confidentiality / Integrity / Availability	The applicant shall perform a risk assessment in accordance to Risk Management policies and procedures for every third party or open source software product.

The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the IoT device software. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The documentation of the tests of the security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test. The applicant shall consider the development and test environments when performing risk assessment. The applicant shall include development resources as part of the backup policy.
The development environment use logical or physical separation between production environments.	Confidentiality / Integrity / Availability	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for production environment.
Appropriate measures are taken to identify vulnerabilities introduced in the IoT device during the development process.	Confidentiality / Integrity / Availability	Code reviews shall be regularly performed by qualified personnel or contractors. The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts.
Outsourced developments provide similar security guarantees than in-house developments.	Confidentiality / Integrity / Availability	The applicant shall 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. Internal or external employees of the applicant shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.
A comprehensive test plan for the IoT devices software is established.	Confidentiality / Integrity / Privacy	The applicant shall should have the IoT devices inspected in the last part of manufacturing/delivery and subjected to cybersecurity testing to detect misconfigurations or errors
IoT application protocols should be configured securely and update default configurations.	Confidentiality / Integrity	The applicant should use IoT application protocols (MQTT, AMQP, CoAP) only over TLS or DTLS connections.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that third parties are supported.	Confidentiality / Integrity / Availability	The applicant 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. The reports shall include the complementary subservice organisation controls that are required, together with the controls of the applicant.

Suppliers of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence over the organisation's third party management capabilities including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: i) Protection needs regarding the confidentiality, integrity and availability of information processed, stored, or transmitted by the third party; ii) Impact of a protection breach on the provision of the outsourcing service; iii)The applicant's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives.
A centralized directory of suppliers is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; vii) Security requirements; viii) Beginning of service usage; and ix) Proof of compliance with contractually agreed requirements.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall test the Incident Response Plan/ procedure at least on an annual basis.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall simulate the identification, analysis, and defence of security incidents and attacks on a quarterly basis through appropriate Table-top tests and exercises. The applicant shall review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness. The applicant shall monitor the processing of incident to verify the application of incident management policies and procedures.

Security incidents are documented to and reported in a timely manner to customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow customers to actively approve the solution before automatically approving it after a certain period.
Measures are in place to continuously improve the service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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. 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The service provider shall establish an integrated team of forensic/ incident responder personnel specifically trained on evidence preservation and chain of custody management
Threat modeling is performance for the whole IoT supply chain.	Confidentiality / Integrity	The applicant shall perform threat modeling procedures prior to moving any IoT applications/devices in the suppy chain.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business business continuity and disaster recovery and contigency management and form a Business Continuity Management & Disaster Recoevry team, which is responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. The business continuity and disaster recovery and team shall ensure that sufficient resources are made available for an effective process.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the infrastructure.	Availability	The business impact assessment shall be performed at least annually and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical products and services; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; viii) Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); ix) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and x) Estimation of the resources needed for resumption. The business impact analysis resulting from these policies and procedures shall be conducted and reviewed at regular intervals, at least once a year, or after significant organisational or environment related changes.

A business continuity framework including a business continuity plan and associated contingency plans is available.	Availability	The business continuity plan and contingency plans shall be at least annually performed and cover at least the following aspects: i) Defined purpose and scope, including relevant business processes and dependencies; ii) Accessibility and comprehensibility of the plans for persons who are to act accordingly; iii) Ownership by at least one designated person responsible for review, updating and approval; iv) Defined communication channels, roles and responsibilities including notification of the customer; v) Recovery procedures, manual interim solutions and reference information; vi) Methods for putting the plans into effect; vii) Continuous process improvement; and viii) Interfaces to Security Incident Management. The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the infrastructure are defined and documented.	Confidentiality / Privacy	The applicant shall provide these procedures when requested by a customer. The applicant shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the service.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the IoT devices software.	Privacy	The applicant shall grant its customers contractually guaranteed information and define their audit rights.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions. The applicant shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate applicant's subject matter experts for immediate assessment and action.

Provide customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow the customer to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall track the data request process via a ticketing system.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall document and implement an active monitoring tool of the regulatory Data Protection requirements they need to follow.
Safeguards to satisfy regulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; iii) secure disposal of personal data according to the regulatory Data Protection requirements; iv) keeping a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.

8 Distributed Ledger Technology

Distributed Ledger Technology (or Blockchain) refers to a distributed technology that maintains a continuously growing list of ordered records, called blocks, including blockchain and smart contracts. A DLT is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.

8.1 TAAF Level 1

Objective	Applicable Type(s)	Description
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make access policies and procedures for controlling access to information resources and based on the business and security requirements of the applicant, in which at least the following aspects are covered: i) Parameters to be considered for making access control decisions; ii) Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle; iii) Use of a role-based mechanism for the assignment of access rights; iv) Segregation of duties between managing, approving and assigning access rights; v) Dedicated rules for users with privileged access; and vi) Requirements for the approval and documentation of the management of access rights. The applicant shall link the access control policy with the physical access control policy, to guarantee that the access to the premises where information is located is also controlled.

Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall document policies for managing accounts in which at least the following aspects are described: i) Assignment of unique usernames; and ii) Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type. The applicant 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. The applicant 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. The applicant shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the DLT service that comply with the role and rights concept and with the policies for managing accounts.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement general guidelines with respect to user access review/ recertification.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The applicant shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: i) The selection of mechanisms suitable for every type of account; ii) The protection of credentials used by the authentication mechanism; and iii) The generation and distribution of credentials for new accounts.
Throughout their lifecycle, authentication credentials and nodes' private keys are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: i) Non-reuse of credentials and nodes' key private keys; ii) Recommendations for renewal of passwords; iii) Rules on the required strength of passwords, together with mechanisms to communicate and enforce the rules; and iv) Rules on storage of passwords and keys; Passwords and keys shall be only stored using cryptographically strong hash functions.
Compliance		

The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the blockchain service are defined and documented.	Confidentiality / Privacy	The applicant shall document the legal, regulatory, self-imposed and contractual requirements relevant to the information security of the blockchain service.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the blockchain service.	Privacy	The applicant shall document, communicate, make available and implement policies and procedures for planning and conducting audits and addressing at least the following aspects: i) Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; ii) Activities that may result in malfunctions to breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and iii) Logging and monitoring of activities.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform at regular intervals and at least annually internal audits by subject matter experts to check the compliance of their internal security control systems. The internal audit shall check the compliance with respect to their ISMS and regulatory frameworks. The applicant shall document specifically deviations that are nonconformities from their ISMS and regulatory frameworks including an assessment of their severity, and keep track of their remediation.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall define, communicate and implement policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall define, communicate and implement a Privacy policy outlining the entity's objectives related to confidentiality and how confidential data are maintained. The Privacy Policy is reviewed and updated at least on an annual basis.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The Applicant is shall define, communicate and implement policies and procedures to safeguard, protect, process and retain personal data.
Operational Security		

Policies are defined that ensure the protection against malware attacks in the DLT infrastructure.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures to protect its DLT components from malware, covering at least the following aspects: i) Use of system-specific protection mechanisms; ii) Operating protection programs on DLT components.
Policies are defined to govern logging and monitoring events on DLT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall document, communicate and implement policies and procedures that govern the logging and monitoring of events on system components.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the DLT components.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for data backup and recovery.
Appropriate safeguards to ensure processing integrity are in place.		The applicant shall document, communicate and implement policies and procedures to ensure that appropriate safeguards and controls are in place to ensure processing integrity.
Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The applicant shall document, communicate and implement policies and procedures related to the physical access control to the security areas. The access control policy shall require at least one authentication factor for accessing any non-public area. The access control policy shall describe the physical access control derogations in case of emergency. The applicant shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to these perimeters. The applicant shall protect security perimeters with security measures to detect and prevent unauthorised access in a timely manner.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall document, communicate, and implement policies and procedures concerning work in non-public areas.

The equipment used in the applicant’s premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The applicant shall document, communicate, and implement policies and procedures concerning the Physical Security controls and safeguards in place. The applicant shall use encryption on removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The applicant shall document and communicate and implement policies and procedures outlining security requirements related to external and environmental threats, addressing the following risks in accordance with the applicable legal and contractual requirements: i) Faults in planning; ii) Unauthorised access; iii) Insufficient surveillance; iv) Insufficient air-conditioning; v) Fire and smoke; vi) Water; vii) Power failure; and viii) Air ventilation and filtration.
Human Resources		
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity of all internal and external employees of the applicant with access to vendor, third party or customer data or DLT components under the applicant’s responsibility, or who will have access in the production environment shall be reviewed before commencement of employment in a position.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define specific policies/ procedures that communicates to internal and external employees their ongoing responsibilities relating to information security when their employment is terminated or changed. The applicant shall apply a specific procedure to revoke the access rights and process appropriately the accounts and assets of internal and external employees when their employment is terminated or changed.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a security awareness and training program that covers basic Information Security principles such as but not limited to: i) Handling system components used in the production environment in accordance with applicable policies and procedures; ii) Handling data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; iii) Information about the current threat situation; and iv) Correct behaviour in the event of security incidents. The applicant shall review their security awareness and training program based on changes to policies and instructions and the current threat situation.
Change and Configuration Management		
Policies and procedures are defined to control changes to blockochain services and nodes.	Confidentiality / Integrity / Availability / Accountability	The applicant shall document, implement, and communicate policies and procedures for change management of the DLT components and nodes.
Changes to the DLT infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.
Changes to the DLT infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are tested prior to deployment.

Changes to the blockchain infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall follow the documented Change Management policy and procedures to ensure that all changes are performed by authorized accounts.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall document, communicate and implement information handling policies and procedures to protect the lifecycle of information.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall document, communicate and implement information/ data classification polies and procedures to enforce appropriate safeguard and controls as per the confidentiality of data.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for establishing the strategy and guidelines to ensure business continuity and disaster recovery and contigency management.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the blockchain infrastructure.	Availability	The applicant shall document, communicate and implement policies and procedures for performing a business impact assessment to determine the impact of any malfunction to the blockchain infrastructure.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures according technical and organisational safeguards to ensure a fast, effective and proper response to all known security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant 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.

Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The applicant shall document, communicate and implement a procedure to archive all documents and evidence that provide details on security incidents. The applicant 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.
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of vendor, third party or customer data processed, stored or transmitted in the DLT infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define a risk assessment methodology to be followed on its DLT infrastructure. The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the DLT service and are in the area of responsibility of the applicant: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the DLT components and nodes.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall stay informed about current threats and vulnerabilities via a documented Threat Modelling process.
Information security is considered in project management and a security governance model.	Confidentiality / Integrity / Availability / Privacy	The applicant shall have a documented an Information Security Policy/ process/ guidelines that outlines the security governance model and the need to include information security in the project management of all projects that may affect the service, regardless of the nature of the project.
Risk Management		

Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall document risk management policies and procedures for the following aspects: i) Identification of risks associated with the loss of confidentiality, integrity, availability (CIA triad); ii) authenticity of information within the scope of the ISMS and assigning risk owners iii) Analysis of the probability and impact of occurrence and determination of the level of risk; iv) Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; v) Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and vi) Documentation of the activities implemented to enable consistent, valid and comparable results.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall implement the policies and procedures covering risk assessment on the entire perimeter of the DLT infrastructure. The applicant shall make the results of the risk assessment available to relevant stakeholders.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of DLT infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures according to the technical and organisational measures for the secure development of the DLT infrastructure. The policies and procedures for secure development shall consider information security from the earliest phases of design.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall define safeguards and guidelines with respect to Software Development Life Cycle, to ensure that the confidentiality and integrity of the source code is adequately protected at all stages of development.
Appropriate measures are taken to identify vulnerabilities introduced in the DLT service during the development process.	Confidentiality / Integrity / Availability	The applicant shall define appropriate safeguards or guidelines to check the for vulnerabilities that may have been integrated into the DLT service during the development process. The procedures for identifying vulnerabilities shall be integrated in the development process.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to DLT network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures outlining technical safeguards and guidelines that are suitable to promptly detect and respond to DLTnetwork-based attacks and to ensure the protection of information and information processing systems.

Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall document, communicate, and implement policies and procedures that include technical and organizational safeguards for encryption and key management in which at least the following aspects are described: i) Usage of strong encryption procedures and secure network protocols ii) Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys iii) Consideration of relevant legal and regulatory obligations and requirements.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	Procedures and technical safeguards for secure key management shall be defined and followed by the applicant.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that vendors and third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring vendors and third parties whose products or services contribute to the provision of the DLT infrastructure. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall document, communicate and implement policies and procedures for controlling and monitoring vendors and third parties whose products or services contribute to the provision of the DLT infrastructure. The applicant shall document, communicate and implement third party questionnaires to be used for the review and monitoring of the security controls of third parties.
A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall maintain a directory for controlling and monitoring the vendors or third parties who contribute to the delivery of the blockchain service.
Asset Management		

The applicant has established procedures for inventorying assets, including all DLT infrastructure components to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall define an Asset Management Policy for maintaining an inventory of DLT assets. The applicant shall periodically perform and update the asset mapping of DLT components based on the Asset Management Policy.
ITA Description, Communication		
The applicant shall ensure that certain information are communicated to the customers or users of the DLT service.	Confidentiality / Integrity / Availability	The applicant shall ensure that at least the following controls are in place: i) any restrictions of use of the system should be made available to the user upon accessing the main login pages of the system; ii) ommitments are communicated to external users, as appropriate, and the commitments and related requirements are communicated to internal system users to enable them to carry out their responsibilities; iii) the responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties; iv) internal and external users have been provided with information on how to report security, availability, processing integrity, confidentiality and protection of personal data failures, incidents, concerns, and other complaints to appropriate personnel; v) system changes that affect internal and external users' responsibilities or the applicant's commitments and system requirements relevant to security, availability, processing integrity, confidentiality and protection of personal data are communicated to those users in a timely manner; vi) all communications should be made available in English.
ITA Description, Formal Documentation		
The applicant shall ensure that the design doucmentation of the system is communicated to customers or users of the DLT service.	Confidentiality / Integrity / Availability	Information regarding the design and operation of the system and its boundaries (possibly through logical and physical architecture diagrams, design documentation, API documentation, etc.) has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation; and
Platform Implementation		

The applicant has taken the necessary measures to imlemenent the DLT infrastructure in line with the Blueprint submitted to the Lead Authority.	Confidentiality / Integrity / Availability	The applicant shall take the necessary measures to implement the DLT service in line with the Blueprint (or equivalent) submitted to the Lead Authority.

8.2 TAAF Level 2

Objective	Applicable Type(s)	Description
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the effectiveness of access request policies and procedures for at least: i) Normal access requests; ii) Privileged access requests; iii) emergency access requests; and iv) external employees' access request.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall define and implement an automated mechanism to block user accounts after a certain number of failed authentication attempts or two-moth inactivity. The limits on authentication attempts used in mechanism for user accounts under the responsibility of the applicant shall be based on the risks on the accounts, associated access rights and authentication mechanisms The applicant 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.

The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The review defined shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. The applicant handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. The applicant shall perform periodic access reviews on applications of medium/ high criticality rating on a bi-annual basis.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	Privileged access rights shall be personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks. 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. The applicant shall require strong authentication for accessing the administration interfaces used by the applicant.
Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to all environments of the applicant shall be authenticated, including non-production environments. Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security.
Throughout their lifecycle, authentication credentials and nodes' private keys are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	When creating credentials and keys, compliance with specifications is enforced automatically as far as technically possible. The credential associated to a personal account should be changed on bi-monthly basis and when the credential is changed or renewed, the person associated to that account shall be notified. 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.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the blockchain service are defined and documented.	Confidentiality / Privacy	The applicant shall document and implement procedures and measure its effectiveness for complying to these contractual requirements.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the blockchain service.	Privacy	The applicant 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.

Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Identified vulnerabilities and deviations shall be subject to risk assessment in accordance with the risk management procedure and follow-up measures are defined and tracked. The applicant shall inform customers for potential deviations and identified vulnerabilities.
Provide vendors, third parties or customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow any vendors, third parties or customers to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options.
Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall provide evidence on the followed policies and procedures to handle personal data requests.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall ensure that the Privacy policy is signed by all new internal and external employees upon onboarding. The applicant shall provide evidence for all controls in place that are applicable to the regulatory Data Protection requirements.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; and iii) secure disposal of personal data according to the regulatory Data Protection requirements.
Operational Security		
Policies are defined that ensure the protection against malware attacks in the DLT infrastructure.	Confidentiality / Integrity / Availability	The applicant 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.

Policies are defined to govern logging and monitoring events on DLT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; and v) Time synchronisation of DLT components.
Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Regular identification of vulnerabilities; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted; and iii) Access to the backed-up data and the execution of restores is performed only by authorised persons.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall provide evidence on the operational effectiveness of monitoring their data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The restore tests shall assess if the specifications for the RTO and RPO agreed are met. Any deviation from the specification during the restore test shall be reported to the applicant's responsible person for assessment and remediation.
Appropriate safeguards to ensure processing integrity are in place.		The applicant shall provide evidence on actions that ensure the operational effectiveness of the integrity processing safeguards and shall include at least the following: i) data inputs are measured and recorded completely, accurately, and timely to meet the Applicant's processing integrity commitments; ii) data inputs are measured and recorded completely, accurately, and timely to meet the Applicant's processing integrity commitments and system requirements; and iii) controls to detect processing errors to meet the Applicant's processing integrity commitments and system requirements.

Physical Security		
Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall require at least two authentication factors are used for access to sensitive areas and to areas hosting system components that process vendor, third party or customer data. The access control policy shall include measures to individually track visitors and third-party personnel during their work in the premises and buildings, identified as such and supervised during their stay. The access control policy shall include logging of all accesses to non-public areas that enables the applicant to check whether only defined personnel have entered these zones.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The policies and procedures shall include a clear screen policy and a clear desk policy for documents and removable media.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall be based on criteria which comply with established rules of DLT. The applicant shall provide at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience. The applicant shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises.
Human Resources		
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The extent of the competency and integrity review (screening) of all internal and external employees shall be proportional to the business context, the sensitivity of the information that will be accessed by the employee, and the associated risks. The competency and integrity of internal and external employees of the applicant shall be reviewed before commencement of employment in a position with a higher risk classification.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall monitor the effectiveness of the policies/ procedures that change/ revoke accounts and logical access rights when the employment of an internal or external employee is terminated or changed. A checklist for the return/ change of assets should be followed by HR or the IT departments when the employment of an internal or external employee is terminated or changed.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties. The applicant shall update their security awareness and training program at least annually. The applicant shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group. The applicant shall measure and evaluate the learning outcomes achieved through the awareness and training programme.
Change and Configuration Management		
Policies and procedures are defined to control changes to blockochain services and nodes.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; and iv) Requirements for the documentation of changes in the system, operational and user documentation.

Changes to the DLT infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The applicant shall define the testing scope prior to deployment. The applicant shall include safeguards that guarantee the confidentiality of the data during the whole process. The applicant 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.
Changes to the DLT infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall provide sufficient evidence on the obtained approvals that were gathered prior to deployment.
Changes to the blockchain infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall define roles and rights for the authorised personnel or blockchain components who are allowed to make changes to the service in the production environment and also utilise version controls. All changes to blockchain service in the production environment shall be logged and shall be traceable back to the individual or system component that initiated the change.
Information Protection		
Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over the applicable controls that correspond to the data handling policies and procedures, which should include controls for all data life cycle phases: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall classify all data according to the data classification policies and procedures on both structured and unstructured data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place.
The organisation shall manage the inventory of its sensitive data and data owners.	Confidentiality / Privacy	The applicant maintains an inventory of sensitive data assets. Data ownership has been defined for sensitive data elements.
Business Continuity		

Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business continuity and disaster recovery and contigency 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.
Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the blockchain infrastructure.	Availability	The business impact assessment shall be performed on a periodic basis and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical components; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; and viii) Determination of time targets for the resumption of critical components within the maximum acceptable time period (RTO); The business impact analysis resulting from these policies and procedures shall be reviewed at least once a year, or after significant organisational or environment related changes.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall inform the customers affected by security incidents in a timely and appropriate manner. The applicant shall establish a Computer Emergency Response Team (CERT), which contributes to the coordinated resolution of security incidents.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall maintain a catalogue (Incident Classification Matrix) that clearly identifies the security incidents that affect customer data, and use that catalogue to classify incidents. 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. The applicant shall regularly measure, analyse and assess the incident handling capabilities via Table-top exercises with which incidents are handled to verify their continued suitability, appropriateness and effectiveness.

Security incidents are documented to and reported in a timely manner to vendors, third parties or customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall continuously report on security incidents to affected vendors, third parties or customers until the security incident is closed and a solution is applied and documented, in accordance to the defined SLA and contractual agreements. The applicant shall inform its customers about the actions taken, according to the contractual agreements. The applicant shall define, make public and implement a single point of contact to report security events and vulnerabilities
Measures are in place to continuously improve the DLT service from experience learned in incidents.	Confidentiality / Integrity	The applicant 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 The applicant shall only contract supporting external bodies that are qualified incident response service providers or government agencies.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The documents and evidence shall be archived in a way that could be used as evidence in court. When the applicant requires additional expertise in order to preserve the evidences and secure the chain of custody on a security incident, the applicant shall contract a qualified incident response service provider only.
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant's ISMS shall be based in accordance to ISO/IEC 27001.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of vendor, third party or customer data processed, stored or transmitted in the DLT infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the applicant's DLT infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; and iii) Operation of the DLT components and nodes. The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions.

The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain contacts with the competent authorities in terms of information security and relevant technical groups to stay informed about current threats and vulnerabilities.
Information security is considered in project management and a security governance model.	Confidentiality / Integrity / Availability / Privacy	All roles and responsibilities within he security governance model are followed by the applicant. The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the DLT service, regardless of the nature of the project.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of DLT components, potential threats and vulnerabilities, mitigation approach and residual risk levels.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their on DLT infrastructure and monitor the remediation of the risks and revise the risk assessment results accordingly.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans.
Development of Information Systems		

Policies are defined to define technical and organisational measures for the development of DLT infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices.
The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the DLT infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The applicant shall design documentation for security features, including a specification of expected inputs, outputs and possible errors, as well as a security analysis of the adequacy and planned effectiveness of the feature. The tests of the security features shall cover all the specified inputs and all specified outcomes, including all specified error conditions.
Appropriate measures are taken to identify vulnerabilities introduced in the DLT service during the development process.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the security safeguards in line with the Blueprint submitted to the Authority that include but are not limited to the following aspects: i) Static Application Security Testing; ii) Dynamic Application Security Testing; iii) Code reviews by subject matter experts; and iv) Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their DLT service.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to DLT network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall feed into a SIEM (Security Information and Event Management) system, all data from the technical safeguards implemented so that countermeasures regarding correlating events can be initiated.
Cryptography and Key Management		

Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of cryptography controls in place esnsuring that all blockcain service servers and nodes are be encrypted at rest.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	The applicant shall follow the following measures with respect to key management: i) Generation of keys for different cryptographic DLT components and applications; ii) Issuing and obtaining public-key certificates; iii) Provisioning and activation of the keys; iv) Secure storage of keys including description of how authorised users get access; v) Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; vi) Handling of compromised keys; and vii) Withdrawal and deletion of keys.
Procurement Management		
Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that vendors and third parties are supported.	Confidentiality / Integrity / Availability	The applicant shall provide evidence on the following aspects related to third party risk management: i) Requirements for the assessment of risks resulting from the procurement of vdenros and third-party services; ii) Requirements for the classification of vendros and third parties based on the risk assessment by the applicant; iii) Information security requirements for the processing, storage, or transmission of information by vendors and third parties based on recognized industry standards; iv) Information security awareness and training requirements for staff; v) Applicable legal and regulatory requirements; vi) Requirements for dealing with vulnerabilities, security incidents, and malfunctions; vii) Specifications for the contractual agreement of these requirements; viii) Specifications for the monitoring of these requirements.

Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment of its vendors and thrid parties in accordance with the policies and procedures for the control and monitoring of vendors and third parties. The applicant 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. The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.
A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory of vendors and third parties for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; and viii) Beginning of service usage.
Asset Management		
The applicant has established procedures for inventorying assets, including all DLT infrastructure components to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	An asset inventory or asset Register shall be maintained and periodically updated by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle. The information recorded with assets shall include the measures taken to manage the risks associated to the DLT components and the data it contains throughout its life cycle.
ITA Description, Communication		

The applicant shall ensure that certain information are communicated to the customers or users of the DLT service.	Confidentiality / Integrity / Availability	The applicant shall ensure that at least the following controls are in place: i) any restrictions of use of the system should be made available to the user upon accessing the main login pages of the system; ii) ommitments are communicated to external users, as appropriate, and the commitments and related requirements are communicated to internal system users to enable them to carry out their responsibilities; iii) the responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties; iv) internal and external users have been provided with information on how to report security, availability, processing integrity, confidentiality and protection of personal data failures, incidents, concerns, and other complaints to appropriate personnel; v) system changes that affect internal and external users' responsibilities or the applicant's commitments and system requirements relevant to security, availability, processing integrity, confidentiality and protection of personal data are communicated to those users in a timely manner; vi) all communications should be made available in English.
ITA Description, Formal Documentation		
The applicant shall ensure that the design doucmentation of the system is communicated to customers or users of the DLT service.	Confidentiality / Integrity / Availability	Information regarding the design and operation of the system and its boundaries (possibly through logical and physical architecture diagrams, design documentation, API documentation, etc.) has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation; and
Platform Implementation		
The applicant has taken the necessary measures to imlemenent the DLT infrastructure in line with the Blueprint submitted to the Lead Authority.	Confidentiality / Integrity / Availability	The applicant shall take the necessary measures to implement the DLT service in line with the Blueprint (or equivalent) submitted to the Lead Authority.

8.3 TAAF Level 3

Objective	Applicable Type(s)	Description
Identity, Authentication and Access Control Management		
Policies and procedures for controlling the access to information resources are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall provide evidence on the use of an automated ticketing tool that supports all user access requests.
Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.	Confidentiality / Integrity / Accountability	The applicant shall base its access control policy on the use of a role-based access control model. The applicant shall document a Segregation of Duties Matrix with respect to the defined roles of the organisation. The applicant shall provide a sample of privileged users access rights to validate that no toxic combinations are present with reference to the Segregation of Duties Matrix. The applicant shall perform evidence on periodic access review on a sample of employees/ administrators. The applicant shall provide evidence of disabled access rights of Leavers and Movers' employees.
Accounts that are inactive for a long period of time or that are subject to suspicious activity are appropriately protected to reduce opportunities for abuse.	Confidentiality / Integrity / Accountability	The applicant shall implement the process on all user accounts under its responsibility. The applicant shall automatically monitor the implemented automated mechanisms. The applicant shall automatically monitor the environmental conditions of authentication attempts and flag suspicious events to the corresponding user or to authorized persons.
The purpose of the user accounts of all types and their associated access rights are reviewed regularly.	Confidentiality / Integrity / Accountability	The applicant shall perform the user access rights via the use of an automated access review/ recertification tool.
Privileged access rights and the user accounts of all types to which they are granted are subject to additional scrutiny.	Confidentiality / Integrity / Accountability	The applicant must revise every six (6) months the list of employees who are responsible for a technical account within its scope of responsibility. The applicant shall maintain an automated inventory of the user accounts under its responsibility that have privileged access rights.

Adequate authentication mechanisms are used in to be granted access to any environment and when needed within an environment.	Confidentiality / Integrity / Accountability	The access to the production environment of the applicant shall require strong authentication. The access to all environments of the applicant containing data shall require strong authentication.
Throughout their lifecycle, authentication credentials and nodes' private keys are protected to ensure that their use provides a sufficient level of confidence that the user of a specific account has been authenticated.	Confidentiality / Integrity / Accountability	The applicant 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. Passwords and private keys of administrator accounts should be stored on logical key vaults or hardware security modules.
Compliance		
The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the blockchain service are defined and documented.	Confidentiality / Privacy	The applicant shall provide these procedures when requested by a vendor, third party or customer. The applicant shall document and implement an active monitoring of the legal, regulatory and contractual requirements that affect the blockchain service.
Conditions are defined that allow audits to be conducted in a way that facilitates the gathering of evidence while minimizing interference with the delivery of the blockchain service.	Privacy	The applicant shall grant its vendors, third parties or customers contractually guaranteed information and define their audit rights.
Subject matter experts regularly check the compliance of the Information Security Management System (ISMS) to relevant and applicable legal, regulatory, self-imposed or contractual requirements.	Confidentiality / Integrity / Availability / Privacy	Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and instructions. The applicant shall implement automated monitoring to identify vulnerabilities and deviations, which shall be automatically reported to the appropriate applicant's subject matter experts for immediate assessment and action. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal audits.
Provide vendors, third parties or customers with choices about the location of the data and of its processing.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow the vendors, third parties or customers to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. All commitments regarding locations of data processing and storage shall be enforced by the DLT service architecture.

Personal Data requests are handled and tracked through a formal procedure based on the applicable Data Protection Requirements (e.g. GDPR, UK-GDPR and CCPA).	Confidentiality / Privacy	The applicant shall track the data request process via a ticketing system.
The Product Privacy Policy - based on the applicable Data Protection Requirements (e.g.: GDPR, UK-GDPR, CCPA) is documented, communicated and implemented to all interested parties.	Confidentiality / Privacy	The applicant shall document and implement an active monitoring tool of the regulatory Data Protection requirements they need to follow.
Safeguards to satisfy rgulatory requirements related to processing and protection of personal data.	Confidentiality / Privacy	The policies and procedures shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) restriction of processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data; ii) secure retention of personal data; iii) secure disposal of personal data according to the regulatory Data Protection requirements; iv) keeping a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.
Operational Security		
Policies are defined that ensure the protection against malware attacks in the DLT infrastructure.	Confidentiality / Integrity / Availability	The applicant shall provide evidence of the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces. The applicant shall update the anti-malware products at the highest frequency that the vendors actually offer.
Policies are defined to govern logging and monitoring events on DLT components.	Confidentiality / Integrity / Availability / Privacy / Accountability	The policies and procedures shall dictate actions to ensure the operational effectiveness of at least the following aspects: i) Definition of events that could lead to a violation of the protection goals; ii) Specifications for activating, stopping and pausing the various logs; iii) Information regarding the purpose and retention period of the logs; iv) Define roles and responsibilities for setting up and monitoring logging; v) Time synchronisation of DLT components; and vi) Compliance with legal and regulatory frameworks. The Applicant shall implement a centralized logging repository mechanism hosted in Malta that is available 24/7 relevant to the DLT infrastructure.

Vulnerabilities in the system components used in the infrastructure are identified and addressed in a timely manner.	Confidentiality / Integrity / Availability	The applicant shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities. The policies and procedures for backup and recovery shall dictate actions that ensure the operational effectiveness of at least the following aspects: i) Automated identification of vulnerabilities through a commercial tool; ii) Assessment of the severity of identified vulnerabilities; iii) Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and iv) Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.
Policies define how measure for data backups and recovery that guarantee the availability of data while protecting its confidentiality and integrity.	Integrity / Availability	The applicant shall provide evidence on actions that ensure the operational effectiveness of the data back-up and recovery policies and procedures and shall include at least the following aspects: i) The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); ii) Data is backed up in encrypted, state-of-the-art form; iii) Access to the backed-up data and the execution of restores is performed only by authorised persons; and iv) Tests of recovery procedures.
The proper execution of data backups is monitored.	Integrity / Availability	The applicant shall configure a portal for automatically monitoring their scheduled data backups.
The proper restoration of data backups is regularly tested.	Integrity / Availability	The applicant shall inform the DLT service vendors and thrid parties or customers or users, at their request, of the results of the recovery tests. Recovery tests shall be aligned withapplicant’s business continuity management requirements.
Appropriate safeguards to ensure processing integrity are in place.		The applicant shall provide evidence on actions that ensure the operational effectiveness of the integrity processing safeguards and shall include at least the following: i) data inputs are measured and recorded completely, accurately, and timely to meet the Applicant's processing integrity commitments; ii) data inputs are measured and recorded completely, accurately, and timely to meet the Applicant's processing integrity commitments and system requirements iii) controls to detect processing errors to meet the Applicant's processing integrity commitments and system requirements; and iv) current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the Applicant's availability commitments and system requirements.
Physical Security		

Physical access through the security perimeters are subject to access control measures that match each zone's security requirements and that are supported by an access control system.	Integrity / Accountability	The access control policy shall describe the time slots and conditions for accessing each area according to the profiles of the users. The logging of accesses shall be automatically monitored and reviewed on an annual basis.
There are specific rules regarding work in non-public areas, to be applied by all internal and external employees who have access to these areas.	Integrity	The applicant shall define a mapping between activities and zones that indicates which activities may/shall not/shall be performed in every security area. The applicant shall define a mapping between assets and zones that indicates which assets may/shall not/shall be used in every security area.
The equipment used in the applicant's premises and buildings are protected physically against damage and unauthorized access by specific measures.	Confidentiality / Integrity / Availability	The procedures shall include a procedure to check the protection of power and communications cabling, to be performed and reviewed bia the Information Security Officer or Physical Security Officer at least every two years, as well as in case of suspected manipulation by qualified personnel. Policies and procedures shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site. The applicant shall provide evidence over the effectiveness of the physical controls and safeguards in place. The applicant shall ensure that any back-up equipment containing a media with vendor, third party or customers data can be returned only if the data are stored on it is encrypted or has been destroyed beforehand using a secure deletion mechanism.
Data centres, are protected against external and environmental threats.	Integrity / Availability	The security requirements for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime. The security requirements for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually.
Human Resources		
The competency and integrity of all internal and external employees are verified prior to commencement of employment in accordance with local legislation and regulation by the applicant.	Confidentiality / Integrity / Availability / Privacy / Accountability	The competency and integrity review (screening) of internal and external employees of the applicant shall be conducted for the employees in all positions.

Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long.Upon termination or change in employment, all the access rights of the employee are revoked or appropriately modified, and all accounts and assets are processed appropriately	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the logical access rights of users and assets of internal or external employees.
The applicant operates a security awareness and training program, which is completed by all internal and external employees of the applicant on a regular basis.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall automatically monitor the completion of the security awareness and training program. The applicant shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme. The applicant shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks.
Change and Configuration Management		

Policies and procedures are defined to control changes to blockochain services and nodes.	Confidentiality / Integrity / Availability / Accountability	The change management policies and procedures shall cover at least the following aspects: i) 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; ii) Requirements for the performance and documentation of tests; iii) Requirements for segregation of duties during planning, testing, and release of changes; iv) Requirements for the proper information of blockchai service vendors and third parties or customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; v) Requirements for the documentation of changes in the system, operational and user documentation; and vi) Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.
Changes to the DLT infrastructure are tested before deployment to minimize the risks of failure upon implementation.	Confidentiality / Integrity / Availability	The tests performed any change before its deployment shall include tests on both a development environment, as well as testing environment. The applicant shall document and implement a procedure that ensures the integrity of the test data used in pre-production. The applicant shall perform penetration testing on DLT components that are internet-facing. Before deploying changes on a system component, the applicant shall perform regression testing on other components of the DLT infrastructure that depend on that system component to verify the absence of undesirable effects. The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the DLT infrastructure are approved before being deployed in the production environment.	Confidentiality / Integrity / Availability / Accountability	The applicant shall monitor the definition and execution of the tests relative to a change, as well as the remediation or mitigation of issues though the use of a centralized solution.
Changes to the blockchain infrastructure are performed through authorized accounts and traceable to the person or system component who initiated them.	Confidentiality / Accountability	The applicant shall automatically monitor the logs changes in the production environment to ensure that the principle of non-repudiation is maintained.
Information Protection		

Information handling policies and procedures are documented to ensure information protection.	Confidentiality / Privacy	The applicant shall provide evidence over applicable controls that correspond to the handling policies and procedures, which should include specific for all data life cycle phases according to the data classification policies and procedures: i) data creation; ii) data use and handling; iii) data retention; and iv) data disposal and destruction.
Information/ data classification policies and procedures are documented to ensure that appropriate controls are enforced as per the confidentiality of information.	Confidentiality / Privacy	The applicant shall use data labelling tool, which shall be consistently performed across most BUs for sensitive, unstructured data in accordance with data classification policies. Approved storage locations have been identified and configured for automatic data labelling as per the data classification policies and procedures, whilst data tagging is not performed on legacy data.
Information discovery capabilities are in place for both scanning internal unstructured and structured data.	Confidentiality / Privacy	The applicant shall utilise an automated tool for the discovery of its sensitive data at-rest and enhanced controls are in place. The applicant shall enforce a CASB solution that will allow expand the discovery capabilities of sensitive data on sanctioned third party cloud apps.
The organisation shall manage the inventory of its sensitive data and data owners.	Confidentiality / Privacy	The applicant maintains an inventory of information assets is maintained and assets are classified by the type of data contained and the relative risk. The inventory management is automated via the use of a centralized dashboard of a discovery tool.
Business Continuity		
Responsibilities are assigned inside the applicant organisation to ensure that sufficient resources can be assigned to define and execute the business continuity plan and that business continuity-related activities are supported.	Confidentiality / Integrity / Availability	The applicant shall name (a member of) top management as the process owner of business business continuity and disaster recovery and contigency management and form a Business Continuity Management & Disaster Recoevry team, which is responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines. The business continuity and disaster recovery and team shall ensure that sufficient resources are made available for an effective process.

Business continuity policies and procedures cover the determination of the impact of any malfunction or interruption to the blockchain infrastructure.	Availability	The business impact assessment shall be performed at least annually and consider at least the following aspects: i) Possible scenarios based on a risk analysis; ii) Identification of critical products and services; iii) Identification of dependencies, including processes (including resources required), applications, business partners and third parties; iv) Identification of threats to critical components; v) Identification of effects resulting from planned and unplanned malfunctions and changes over time; vi) Determination of the maximum acceptable duration of malfunctions; vii) Identification of restoration priorities; viii) Determination of time targets for the resumption of components within the maximum acceptable time period (RTO); ix) Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and x) Estimation of the resources needed for resumption. The business impact analysis resulting from these policies and procedures shall be conducted and reviewed at regular intervals, at least once a year, or after significant organisational or environment related changes.
Incident Management		
A policy is defined to respond to security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability / Privacy	The applicant shall test the Incident Response Plan/ procedure at least on an annual basis.
A methodology is defined and applied to process security incidents in a fast, efficient and orderly manner.	Confidentiality / Integrity / Availability	The applicant shall simulate the identification, analysis, and defence of security incidents and attacks on a quarterly basis through appropriate Table-top tests and exercises. The applicant shall review the results of the Table-top exercises by accountable departments to initiate continuous improvement actions and verify their effectiveness. The applicant shall monitor the processing of incident to verify the application of incident management policies and procedures.
Security incidents are documented to and reported in a timely manner to vendors, third parties or customers.	Confidentiality / Integrity / Availability / Privacy	The applicant shall allow customers to actively approve the solution before automatically approving it after a certain period.

Measures are in place to continuously improve the DLT service from experience learned in incidents.	Confidentiality / Integrity	The applicant shall define, implement and maintain a knowledge repository of security incidentsand 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. 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.
Measures are in place to preserve information related to security incidents.	Confidentiality / Integrity / Accountability	The service provider shall establish an integrated team of forensic/ incident responder personnel specifically trained on evidence preservation and chain of custody management.
Organisation of Information Security		
The applicant operates an information security management system (ISMS). The scope of the ISMS covers the applicant's organisational units, locations and processes.	Confidentiality / Integrity / Availability / Privacy / Accountability	The applicant shall have obtained a valid ISO/IEC 27001 certification.
Conflicting tasks and responsibilities are separated based on an risk assessment to reduce the risk of unauthorised or unintended changes or misuse of vendor, third party or customer data processed, stored or transmitted in the DLT infrastructure.	Confidentiality / Integrity / Availability / Privacy / Accountability	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the DLT infrastructure: i) Administration of rights profiles, approval and assignment of access and access authorisations; ii) Development, testing and release of changes; iii) Operation of the DLT components and nodes.; The applicant shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions. The applicant shall automatically monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.
The applicant stays informed about current threats and vulnerabilities by maintaining the cooperation and coordination of security-related aspects with relevant authorities and special interest groups. The information flows into the procedures for handling risks and vulnerabilities.	Confidentiality / Integrity / Availability	The applicant shall maintain a list with the competent authorities in terms of information security and relevant technical groups on an bi-annual basis to stay informed about current threats and vulnerabilities that are specific to their sector.

Information security is considered in project management and a security governance model.	Confidentiality / Integrity / Availability / Privacy	All roles and responsibilities within he security governance model are followed by the applicant. The applicant shall perform a risk assessment to assess and treat the risks on any project that may affect the provision of the on DLT service, regardless of the nature of the project. The applicant shall include the review and signoff from the Information Security Officer and any relevant stakeholders holding a security role, prior to the initiation of a new project.
Risk Management		
Risk management policies and procedures are documented and communicated to stakeholders	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence of the Risk Management Register that includes but is not limited to identification of DLT components, potential threats and vulnerabilities, mitigation approach and residual risk levels. The Risk Management Register should be updated at least on an annual basis.
Risk assessment-related policies and procedures are implemented on the entire perimeter of the service.	Confidentiality / Integrity / Availability / Privacy	The applicant shall perform a risk assessment on their on DLT infrastructure and monitor the remediation of the risks and revise the risk assessment results via an automated dashboard or risk compliance solution.
Identified risks are prioritized according to their criticality and treated according to the risk policies and procedures by reducing or avoiding them through security controls, by sharing them, or by retaining them. Residual risks are accepted by the risk owners.	Confidentiality / Integrity / Availability / Privacy	The applicant shall define and implement a plan to treat risks according to their priority level by reducing or avoiding them through security controls, by sharing them, or by retaining them. The risk owners shall formally approve the treatment plan and in particular accept the residual risk via signoff. The risk owners and the Information Security Officer shall review for adequacy the analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, after each revision of the risk assessment and treatment plans. The applicant shall monitor the effectiveness of the risk treatment activities via an automated dashboard or risk compliance solution.
Development of Information Systems		
Policies are defined to define technical and organisational measures for the development of DLT infrastructure throughout its lifecycle.	Confidentiality / Integrity / Availability	The controls under the secure development policies and procedures shall be based on recognised standards and methods with regard to the following aspects: i) Security in Software Development (Requirements, Design, Implementation, Testing and Verification); ii) Security in software deployment (including continuous delivery); iii) Security in operation (reaction to identified faults and vulnerabilities); and iv) Secure coding standards and practices via automated static or dynamic scanning tools.

The development environment takes information security in consideration.	Confidentiality / Integrity / Availability	The applicant shall implement secure development and test environments that makes it possible to manage the entire development cycle of the information system of the DLT infrastructure. The applicant shall use version control to keep a history of the changes in source code with an attribution of changes to individual developers. The documentation of the tests of the security features shall include at least a description of the test, the initial conditions, the expected outcome and instructions for running the test. The applicant shall include development resources as part of the backup policy.
Appropriate measures are taken to identify vulnerabilities introduced in the DLT service during the development process.	Confidentiality / Integrity / Availability	Code reviews shall be regularly performed by qualified personnel or contractors. The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts.
Communication Security		
The applicant has implemented appropriate technical safeguards in order to detect and respond to DLT network based attacks as well as to ensure the protection of information and information processing systems.	Confidentiality / Integrity / Availability	The applicant shall implement technical safeguards to ensure that no anonymous nodes join the DLT network. The applicant shall use different technologies on its technical safeguards to prevent that a single vulnerability leads to the simultaneous breach of several defence lines. Technical safeguards shall be implemented so that automatic countermeasures regarding correlating events are initiated.
Cryptography and Key Management		
Policies and procedures for encryption mechanisms and key management including technical and organisational safeguards are defined, communicated, and implemented, in order to ensure the confidentiality, authenticity and integrity of the information.	Confidentiality / Integrity / Privacy	The applicant shall provide evidence of at least the following aspects of cryptography and key management: i) All blockcain service servers and nodes shall be encrypted at rest; and ii) Strong cryptography and security protocols are used (e.g., TLS, IPsec, SSH, etc.) to safeguard confidential information during transmission.
Appropriate mechanisms for key management are in place to protect the confidentiality, authenticity or integrity of cryptographic keys.	Confidentiality / Integrity	For the secure storage of keys and other secrets used for the administration tasks, the applicant shall use designated key vaults and should rotate the keys on a quarterly basis.
Procurement Management		

Responsibilities are assigned inside the organisation to ensure that sufficient resources can be assigned to ensure that that vendors and third parties are supported.	Confidentiality / Integrity / Availability	The applicant 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. The reports shall include the complementary subservice organisation controls that are required, together with the controls of the applicant.
Vendors and third parties of the applicant undergo a risk assessment to determine the security needs related to the product or service they provide.	Confidentiality / Integrity / Availability / Privacy	The applicant shall provide evidence over the organisation's third party management capabilities including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: i) Protection needs regarding the confidentiality, integrity and availability of information processed, stored, or transmitted by the vendor and third party; ii) Impact of a protection breach on the provision of the outsourcing service; iii)The applicant's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives.
A centralized directory of vendors and third parties is available to facilitate their control and monitoring.	Confidentiality / Privacy	The applicant shall verify and review the directory of vendors and third parties for completeness, accuracy and validity at least annually. The directory shall contain the following information: i) Company name; ii) Address; iii) Locations of data processing and storage; iv) Responsible contact person at the service provider/supplier; v) Responsible contact person at the applicant; vi) Description of the service; vii) Classification based on the risk assessment; vii) Security requirements; viii) Beginning of service usage; and ix) Proof of compliance with contractually agreed requirements.
Asset Management		

The applicant has established procedures for inventorying assets, including all DLT infrastructure components to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Integrity / Availability	The applicant shall automatically monitor the asset inventory via the provisioning of an inventory tool to ensure that all entries on the inventory are up-to-date.
ITA Description, Communication		
The applicant shall ensure that certain information are communicated to the customers or users of the DLT service.	Confidentiality / Integrity / Availability	The applicant shall ensure that at least the following controls are in place: i) any restrictions of use of the system should be made available to the user upon accessing the main login pages of the system; ii) ommitments are communicated to external users, as appropriate, and the commitments and related requirements are communicated to internal system users to enable them to carry out their responsibilities; iii) the responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties; iv) internal and external users have been provided with information on how to report security, availability, processing integrity, confidentiality and protection of personal data failures, incidents, concerns, and other complaints to appropriate personnel; v) system changes that affect internal and external users' responsibilities or the applicant's commitments and system requirements relevant to security, availability, processing integrity, confidentiality and protection of personal data are communicated to those users in a timely manner; vi) all communications should be made available in English.
ITA Description, Formal Documentation		
The applicant shall ensure that the design doucmentation of the system is communicated to customers or users of the DLT service.	Confidentiality / Integrity / Availability	Information regarding the design and operation of the system and its boundaries (possibly through logical and physical architecture diagrams, design documentation, API documentation, etc.) has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation; and
Platform Implementation		

The applicant has taken the necessary measures to imlemenent the DLT infrastructure in line with the Blueprint submitted to the Lead Authority.	Confidentiality / Integrity / Availability	The applicant shall take the necessary measures to implement the DLT service in line with the Blueprint (or equivalent) submitted to the Lead Authority.