



EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme
for cloud services

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use certification@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

ENISA thanks the members of the ad-hoc Working Group (available from https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG02/ahwg02_members), as well as the representatives from the Member States and the European Commission, and the representatives from all the observer organisations who supported ENISA for the establishment of this scheme from March to December 2020.

LEGAL NOTICE

This draft document constitutes a preparatory legal text to be submitted for consultation under article 49 of the Cybersecurity Act (Regulation 2019/881). It represents the preliminary views of ENISA, and may not in any circumstance be regarded as stating of an official position of ENISA or the Commission. It does not constitute a legal act of ENISA or Commission or the ENISA or Commission bodies. No rights can be derived from it. This draft document does not constitute a formal publication of ENISA and does not necessarily represent state-of-the-art; this is a draft version of the candidate EU cybersecurity certification scheme and is solely distributed for consultation according to Article 49.3 of the Cybersecurity Act, and shall not be used for any other purpose. After consultation, ENISA may amend it.

Third-party sources are aimed to be quoted as appropriate, but due to the fact that this is a draft version, there may be a possibility that minor irregularities may be subject to correction. ENISA is not responsible for the content of the external sources including external websites referenced in this document. Flow charts, models, matrixes and statistics are also to be considered under draft status. No rights may be derived from them.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2020. All rights reserved for this draft version. Redistribution or reproduction of this draft candidate EU cybersecurity certification scheme is only allowed for consultation purposes and shall be shared in its entirety. Any other use of this copyright is strictly prohibited.

Copyright for the image on the cover: © Shutterstock

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

TABLE OF CONTENTS

1. A SCHEME FOR CLOUD SERVICES	4
2. SUBJECT MATTER AND SCOPE	8
3. PURPOSE OF THE SCHEME	12
4. USE OF STANDARDS	17
5. ASSURANCE LEVELS	19
6. SELF-ASSESSMENT	27
7. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB	29
8. EVALUATION METHODS AND CRITERIA	31
9. NECESSARY INFORMATION FOR CERTIFICATION	34
10. MARKS AND LABELS	37
11. COMPLIANCE MONITORING	39
12. CERTIFICATE MANAGEMENT	44
13. NON-COMPLIANCE	49
14. NEW VULNERABILITIES	53
15. RECORD RETENTION	56
16. RELATED SCHEMES	57
17. CERTIFICATE FORMAT	59
18. AVAILABILITY OF INFORMATION	60
19. CERTIFICATE VALIDITY	61
20. DISCLOSURE POLICY	62
21. MUTUAL RECOGNITION	64
22. PEER ASSESSMENT	67

23. SUPPLEMENTARY INFORMATION	70
24. ADDITIONAL TOPICS	72
25. FURTHER RECOMMENDATIONS	76
26. REFERENCES	79
ANNEX A: SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES	81
ANNEX B: META-APPROACH FOR THE ASSESSMENT OF CLOUD SERVICES	159
ANNEX C: ASSESSMENT FOR LEVELS SUBSTANTIAL AND HIGH	173
ANNEX D: ASSESSMENT FOR LEVEL BASIC	183
ANNEX E: COMPETENCE REQUIREMENTS FOR CABS	189
ANNEX F: SCHEME DOCUMENT CONTENT REQUIREMENTS	190
ANNEX G: CERTIFICATION LIFECYCLE AND CONTINUED ASSURANCE	218
ANNEX H: PEER ASSESSMENT	222
ANNEX I: TERMINOLOGY	230

1. A SCHEME FOR CLOUD SERVICES

Foreword for Reviewers

This present version of the European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) is a draft version, to be used as basis for an External Review.

The objective of this review is to validate the principles and general organization of the proposed scheme, and to gather feedback on the proposed wording of the sections and annexes.

A foreword like this one is included at the beginning of Chapters and Annexes for which a specific comment is required. In particular, the foreword will mention the level of maturity of the section or annex, and in some cases issues that remain under discussion.

The terminology is not final only defines essential words, and it is complemented by the terminology defined in Annex I: (Terminology).

1.1 INTRODUCTION

Following the request from the European Commission in accordance with Article 48.2 of the Cybersecurity Act¹ (hereinafter referred to as EUCSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) to support the preparation of a candidate EU cybersecurity certification scheme on cloud services.

Based on the outcomes from this AHWG, launched on March 5th, 2020 and composed of twenty (20) selected members representing industry (e.g., cloud service providers, cloud service customers, conformity assessment bodies), as well as around twelve (12) participants from accreditation bodies and EU Member States, regular exchanges with the ECCG and after an internal review, ENISA has consolidated the following candidate scheme.

The candidate EUCS scheme (European Cybersecurity Certification Scheme for Cloud Services), looks into the certification of the cybersecurity of cloud services. The scheme draws from many different sources, the first one being the report of the CSP-CERT Working Group, which was delivered in 2019 and provided a basic framework on which the candidate scheme has been developed.

EUCS supports the three assurance levels in the EUCSA: 'basic', 'substantial' and 'high'. The security requirements on cloud services and on their assessment increase with levels in several dimensions: scope, rigour and depth. The requirements at level 'high' are demanding and close to the state-of-the-art, whereas the requirements at level 'basic' define a minimum acceptable baseline for cloud cybersecurity. That baseline is nevertheless comprehensive, as it covers all major aspects of cloud security. Cloud service providers of any size can use it to demonstrate that they have set up a framework for guaranteeing some security of their customers. The 'substantial' level, in between, will serve to protect business, and may be the level of choice for many applicants and their users.

The candidate scheme targets a specific category of ICT services, so it is naturally based on the ISO/IEC 17065 standard in terms of applicable requirements to CABs performing certification. There are two main standards suitable

¹ REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

for the assessment of the cybersecurity of cloud services, respectively based on the ISO27000 series of standards and on the International Auditing Standards. The scheme defines an assessment approach that is compatible with both approaches, allowing cloud service providers to easily integrate the scheme into their current certification and assurance strategy.

The candidate scheme also defines a simplified assessment methodology for the EUCSA assurance level 'basic'. The methodology is based on a self-assessment performed by the cloud service provider, whose results are then audited by a conformity assessment body. The candidate scheme does not however allow cloud service providers to issue EU statements of conformity.

The security requirements defined in the scheme draw significantly from the German C5 scheme, but they also draw some inspiration from the French SecNumCloud scheme, from the proposals in the CSP-CERT report, and from principles in other schemes used in Europe.

Finally, the EUCS scheme is not a standalone scheme; it is part of the European cybersecurity certification framework. Although it is very different from the first scheme in the framework, EUCC, which focuses on ICT products, there are commonalities, for instance around the organization of compliance monitoring and peer assessments. The EUCS scheme leverages some principles that were first defined in the EUCC scheme, and follows the same general presentation, with 22 chapters that provide answers to the requirements stated in Article 54.1 of the EUCSA, followed by annexes that define in greater details the content of the scheme.

Guidance will also be key to support the adoption of the scheme by providing harmonised interpretation or refinement of requirements established into the candidate EUCS scheme, and the text indicates explicitly where guidance will be most required.

1.2 GLOSSARY

The first sections outline the most important terminology drawn from existing standards, including ISO/IEC 17788, ISO/IEC 27000 and ISO/IEC 17000.

1.2.1 From ISO/IEC 17788

We will reuse the following terminology from ISO/IEC 17788:

Term	Abbreviations	Definition
Application capabilities type		Cloud capabilities type in which the cloud service customer can use the cloud service provider's applications
Cloud capabilities type		Classification of the functionality provided by a cloud service to the cloud service customer , based on resources used.
Cloud computing		Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
Cloud service		One or more capabilities offered via cloud computing invoked using a defined interface.
Cloud service customer	CSC	Party which is in a business relationship for the purpose of using cloud services .
Cloud service customer data		Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service , or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service . NOTE 1 – An example of legal controls is copyright. NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available

Term	Abbreviations	Definition
		data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.
Cloud service derived data		Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer . NOTE – Cloud service derived data includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.
Cloud service provider	CSP	Party which makes cloud services available
Cloud service provider data		Class of data objects, specific to the operation of the cloud service , under the control of the cloud service provider NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.
Cloud service user	User	Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services. NOTE: Examples of such entities include devices and applications.
Infrastructure capabilities type		Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources
multi-tenancy		Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.
on-demand self-service		Feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider .
Platform capabilities type		Cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider .
tenant		One or more cloud service users sharing access to a set of physical and virtual resources.

We will in general not use the terminology from 17788 that is not included in the table above. More specifically, the following terminology should be avoided in the definition of the scheme:

Term	Rationale
XXaaS	These “as a Service” correspond to the cloud service categories, which are too specific. Cloud capabilities types should be used instead in the scheme. In particular, IaaS, PaaS and SaaS should not be used.
Cloud service category	Cloud service categories are too specific and should not be used in the scheme, except when used in their specific meaning.
Cloud service partner	We have not identified a specific need for using the notion of cloud service partner, so it is recommended not to use it in the document.

1.2.2 Specific terminology

The following glossary defines some of the most commonly used terms and abbreviations in this document.

Term	Abbreviation	Definition
Ad hoc working group	AHWG	The working group that supports ENISA in the definition of the certification scheme on cloud services
Conformance Assessment Body	CAB	An entity in charge of the certification of products, services, and processes, typically according to ISO17065.
	CSP-CERT	The Working Group on Certification for Cloud Service Providers, who produced a report in 2019 that provides a starting point for the development of the certification schemes for cloud services.
European Cybersecurity Certification group	ECCG	A group composed of representatives of national cybersecurity certification authorities or other relevant national authorities (EUCSA, Article 62)
	EUCC	The candidate European cybersecurity certification scheme to serve as a successor to the existing SOG-IS
	EUCS	The present candidate European cybersecurity certification scheme for cloud services
Cybersecurity Act	EUCSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
National Cybersecurity Certification Authority	NCCA	A national authority in every EU Member State that is in charge of the oversight of the certification framework in its country, and also in charge of issuing certificates at 'high' level in its own country.
Stakeholder Cybersecurity Certification Group	SCCG	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders

A far more complete terminology of certification and cloud-related terms is included in Annex I: (Terminology), which is used throughout this draft document

2. SUBJECT MATTER AND SCOPE

Foreword for Reviewers

Chapters 2 to 23 follow the same structure. Each one of them provides content related to one of the points raised in Article 54(1). There are 22 such points, numbered (a) to (v), so there are 22 chapters.

Every chapter contains the following sections:

- An excerpt from Article 54 defining the topic to be addressed in the chapter.
- A proposed text, which is the proposed content for the scheme. This content defines scheme rules and requirements, and makes extensive use of “shall” to express a requirement, and “may” to express an option.
- A rationale, starting when available by relevant excerpts from the EU Cybersecurity Act, and providing additional information, reasons for making the choices in the proposed text, and any other additional information deemed necessary.

When reviewing these chapters, the proposed text is the essential part for the review, but comments are also welcome on the rationale, in particular to indicate a potential lack of justification of a given point.

As a rule of thumb, the chapters that do not include a dedicated foreword are typically chapters that are (1) derived from earlier work, typically principles decided early in the spring, or (2) adapted from the EUCC scheme, with some initial review by a few AHWG members. In other cases, the foreword will provide additional information.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

The rest of Article 54 also provides useful information:

2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.
3. Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.
4. In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.



The European cybersecurity certification scheme for cloud services, hereinafter referred to as the EUCS scheme, shall allow for the cybersecurity certification of cloud services according to the criteria and methods defined in Chapter 8 below (Evaluation Methods and Criteria).

The EUCS scheme may cover any type of ICT service, provided that:

- The ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface [ISO17788].
- The ICT service aims at reaching the assurance level corresponding to one of the three levels 'basic', 'substantial' and 'high' of the EUCSA as defined in the EUCS scheme

ICT services matching these criteria will from now be referred to as "cloud services". The EUCS scheme may apply to all cloud services, following some principles:

- The EUCS scheme distinguishes between different categories of cloud services by relying on the cloud capabilities types (infrastructure, platform, application);
- The EUCS scheme aims at establishing the conformity of cloud services to a set of requirements corresponding to one of the assurance levels defined in the EUCS scheme;
- The EUCS scheme aims at making geographical and legal information about the cloud services available and understandable to all users of the scheme to allow to use them as needed.
- The EUCS scheme acknowledges that the responsibility for the security of a cloud service is split between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC), and aims at verifying that this split of responsibility is explicitly and publicly documented by the CSP.
- The EUCS scheme aims at providing sufficient information for making informed security decisions on cloud services to prospects and customers with adequate cybersecurity knowledge, allowing them to fully understand and implement the documentation that defines their responsibility.

Finally, in the evaluation of a cloud service, the EUCS scheme shall support and encourage the reuse of conclusions and evidence from already audited or certified ICT products, ICT processes, and ICT services, in particular those cloud services that have been certified with the EUCS scheme:

- The scheme includes an assessment of the dependencies, in which the assurance information available from subservice organizations is considered and compared to the requirements of the scheme, in particular regarding the required level of assurance (see Annex B: Meta-approach for the assessment of cloud services).
- When a certified composite cloud service relies on a base cloud service certified with the EUCS scheme, the EUCS scheme shall aim at verifying that the recommendations defined in the base cloud service are adequately

applied by the composite cloud service, and included into the recommendations defined for that composite cloud service (see Section 24.4, Composition).

The EUCS scheme also covers additional elements as foreseen by Article 54 of the CSA, under the conditions defined by Chapter 24, Additional Topics:

- The definition of Security Profiles;
- The handling of force majeure cases;
- Rules for the protection of information related to cybersecurity certification;

RATIONALE

Additional information

In the request to prepare the scheme, the Commission asks ENISA to “... prepare a candidate European cybersecurity certification scheme for cloud services.” In addition, the request is justified by the need to “stimulate cloud uptake in Europe” as “cloud computing is an underlying technology for any development in technological fields.”



The core definitions come from ISO/IEC17888. The definition of cloud computing and cloud service as provided in ISO/IEC17888 suit well the objectives of the EUCS scheme, which aims at being a horizontal scheme for a wide range of cloud services. The definition of a cloud service is very generic, as long as it is based on cloud computing, which is defined in ISO/IEC17888 with all the classical properties (scalability, elasticity, shareable resources, self-service and on-demand).

The notion of capability and capability type is central and also defined in ISO/IEC 17788:

3.2.4 cloud capabilities type: Classification of the functionality provided by a cloud service (3.2.8) to the cloud service customer (3.2.11), based on resources used.

NOTE – The cloud capabilities types are application capabilities type (3.2.1), infrastructure capabilities type (3.2.25) and platform capabilities type (3.2.31).

3.2.1 application capabilities type: Cloud capabilities type (3.2.4) in which the cloud service customer (3.2.11) can use the cloud service provider's (3.2.15) applications.

3.2.25 infrastructure capabilities type: Cloud capabilities type (3.2.4) in which the cloud service customer (3.2.11) can provision and use processing, storage or networking resources.

3.2.31 platform capabilities type: Cloud capabilities type (3.2.4) in which the cloud service customer (3.2.11) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider (3.2.15).

Capabilities provide a more precise framework than the classical categories (IaaS, PaaS, SaaS, XXaaS, etc.), allowing a cloud service to precisely define the capabilities that it provides to its customers (e.g., a SaaS service may simply provide application capabilities on top of an already certified infrastructure and platform, or it may provide infrastructure, platform and application capabilities if the CSP uses a cloud computing system built from the ground up).

There are other ways to categorize cloud services, such as the deployment models. ISO/IEC 17788 defines four deployment models, depending on the control and sharing of physical or virtual resources: community cloud, private cloud, public cloud, and hybrid cloud.

For the purpose of the EUCS scheme, we did not identify any specific need to focus on deployment models in addition to cloud capabilities types to categorize cloud services. Nevertheless, although deployment models are not mentioned in the scheme, it does not mean that deployment models can be fully ignored in the evaluation of a cloud service, as the evidence to be provided may differ for some controls or requirements.

About scoping, the most important characteristic of the EUCS scheme is that it is intended to be a horizontal scheme, applying the same criteria to all cloud services, with three levels of assurance. These criteria apply to the design and implementation of the cloud service, including its security features and the essential processes used throughout its lifecycle, in particular for development, deployment and operation.

The EUCS scheme includes a security profile mechanism that allows industries or verticals to define dedicated requirements, but individual cloud service providers are not allowed to remove from or add to the security requirements defined in the EUCS scheme.

In addition, the EUCS scheme does not aim at verifying the compliance of a cloud service to any regulation beyond the EUCSA, and in particular it does not aim at verifying compliance with GDPR². Such compliance will have to be verified using a dedicated certification scheme, and results obtained in the EUCS scheme may be reused in such schemes.

Finally, the EUCS scheme is a technical tool designed to provide information to customers and allow them to make informed decisions. As such, the EUCS scheme does not enforce any restrictions on geographical location of data or processing, or on applicable laws; however, it requires the CSP to be transparent about this information, and to make it publicly available and understandable as part of the information provided with the certificate.

The EUCS scheme recognizes that cloud services are based on complex systems, and that many CSPs will use subservices provided by subservices organizations. Beyond typical security controls on the control and monitoring of suppliers and service providers, the assessment methods therefore include at all levels an assessment of the assurance documentation provided by subservice providers with regards to the requirements of the EUCS scheme.

The EUCS scheme also defines requirements for composition. When a cloud service uses a subservice that has been previously certified in the EUCS scheme, it should be easy to reuse the results from that certification. The requirements related to composition defined in the EUCS scheme apply to both the base cloud service and to the dependent cloud service.

Another important aspect of certification is related to the split of responsibility between the CSP and the CSC (Customer). The fulfilment of the requirements by the CSP's cloud services is evaluated under the assumption that the CSC follows the recommendations provided by the CSP in the cloud service's documentation.

In terms of certification, when a cloud service A relies on another certified cloud service B, it needs to follow the security recommendations provided by cloud service B, or when necessary, to "forward" the recommendations to its own end users.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

3. PURPOSE OF THE SCHEME

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements

(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme;



The EUCS scheme aims at improving the Internal Market conditions, and at enhancing the level of security of a wide range of cloud services, of the cloud capabilities they implement, including application, infrastructure, and platform capabilities.

The EUCS scheme also covers a wide range of security requirements, by offering all three (3) security assurance levels defined in the EUCSA ('basic', 'substantial' and 'high').

Users of the scheme may be:

- cloud service providers (CSPs) who wish to assess the security of their cloud services through third-party certification;
- cloud service customers (CSCs) who wish to benefit from the evidence provided with certified cloud services to make informed decisions related to the security of these cloud services;
- regulatory authorities who wish to include security and assurance requirements on cloud services within their regulations and directives.

These users may use the EUCS scheme:

- to assess how a cloud service, as described by the CSP, meets the requirements of a predefined set of security control objectives and a related set of measures, when used according to security recommendations provided by the CSP;
- to provide CSCs the information required to make informed choices about the procurement and operation of cloud services, and to allow CSCs to use certified cloud services in their own development activities, and to meet their own security compliance requirements;
- to allow regulatory authorities to refer to the scheme in European and national regulations, including criteria based on information defined in the scheme, and to check compliance by verifying the information provided in the certificates stored in the site managed by ENISA.

The EUCS scheme defines rules and mechanisms that may be combined to allow users to reach these objectives:

- three (3) assurance levels (see Chapter 5, Assurance Levels) corresponding to levels 'basic', 'substantial' and 'high' defined in the EUCSA, which can cover cloud services corresponding to a wide range of risk profiles;
- a set of security objectives and requirements (see Chapter 8, Evaluation Methods and Criteria), defining objectives to be met by CSPs for all certified cloud services, further decomposed into requirements mapped to the assurance levels referred to above;
- an assessment meta-approach (see Annex B: Meta-approach for the assessment of cloud services) defining how to use various assessment methods to determine that a cloud service fulfils the requirements assigned to a given assurance level;

- two assessment methods (see Chapter 8, Evaluation Methods and Criteria, Annex C:; Assessment for levels Substantial and High and Annex D:; Assessment for level Basic) defining how to determine that a cloud service fulfils a given set of requirements;
- a set of document templates to be used during the evaluation and review activities (Annex F:; Scheme Document Content requirements) to ensure that the documents released by the CAB and its subcontractors follow the same organization and flow;
- a detailed list of the documents to be made publicly available as part of the certificate package, that may allow scheme users to locate the information they are looking for to make informed decisions;
- a set of rules about the lifecycle of certificates after their issuance, including maintenance and renewal requirements, management of vulnerabilities and complaints, and market surveillance activities, that may allow scheme users to remain informed of the evolution of the security of a given cloud service.

In addition to these technical features, all stakeholders interested in the cybersecurity certification of cloud services will benefit from the following characteristics from the EUCS scheme:

- a scheme harmonized at the European level;
- strong quality guarantees through the use of third-party assessment by accredited bodies, supervision by national authorities, and for the High level, authorization by the national authorities and peer assessment between conformity assessment bodies;
- the flexibility offered by three different assurance levels covering the entire range of assurance introduced in the EUCSA, with the possibility for a certified cloud service to upgrade to a higher level in future evaluation cycles;
- strong transparency guarantees, with security information made publicly available through a centralized web site;
- assurance maintained over time, with regular reassessments, operating effectiveness guarantees at the levels Substantial and High;
- a maintenance framework for the EUCS scheme itself, endorsed by European institutions and Member states, providing strong guarantees on continued operation of the scheme;
- integration in the European cybersecurity certification framework, which will facilitate the reuse of EUCS-certified cloud services in vertical schemes.

The mechanisms defined above provide the means allowing the scheme's intended users to meet their objectives, by providing the conditions required for performing evaluations, issuing and managing certificates, and maintaining the framework and scheme over time.

RATIONALE

Additional input

Recital 74 (excerpt). The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle.

Recital 92 (excerpt). European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended end user.



The scheme's intended users cover all relevant stakeholders in the life cycle of the certificate (production and consumption) and, due to the nature of the scheme, all relevant stakeholders in the life-cycle of the cloud service.

Table 1 and Table 2, below, describe the intended users as stakeholders of the certificate, their role and their use case related to the scheme.

Table 1: Stakeholders involved in the production of certificates

Stakeholder	Role	Use case
Cloud Service Provider	Development	The Development role covers the activities related to the development of the cloud service, including architecture design, hardware and software development, and service design. It also includes processes, in particular the development process.
Cloud Service Provider	Operations	The Operations role covers the activities related to the operation of the cloud service, including procurement, provisioning, update, and other processes. Some processes may be shared with Development, like DevOps (when Development and Operations personnel may be combined in the implementation of shared processes).
Cloud Service Provider	Compliance	The Compliance role covers the activities related to the verification of compliance to standards and regulations, including documentation, self-assessment, interfaces with CABs, and management of EU statements of conformity.
CAB	Evaluation	The Evaluation role for CABs includes all the activities related to the assessment of cloud services and related processes.
CAB	Review and Certification	The Review and Certification role for CABs includes all the activities related to the issuance and management of certificates, including in particular the review of the evaluation and of its results.
NCCA	As a CAB	For level 'high', the NCCA is involved and may perform the tasks of a CAB. This would include at least the Review and Certification role, and it may also include the Evaluation role.
NCCA	Compliance monitoring	NCCAs have a Compliance Monitoring role, to ensure that certified cloud services remain compliant to the requirements of the scheme.
NAB	CAB Accreditation	NABs are not directly involved in the production of certificates, but their role in the accreditation of CABs is essential in the proper operation of the scheme
ENISA	Publicity	ENISA is in charge of publicizing the certificates issued in the context of the scheme, as well as the events associated with these certificates.

Table 2: Stakeholders consuming certificates

Stakeholder	Role	Use case
Cloud Service Customer	Procurement	The Procurement role covers the activities related to the selection of a cloud service, and in particular the definition of the criteria and the assessment of the candidates, leading to the selection.
Cloud Service Customer	Customer Development	The Customer Development role covers the activities related to the development of new products or services on the basis of the certified cloud service, possibly including other cloud services. Developers will in particular rely on the recommendations provided with the certified cloud service.
Cloud Service Customer	Customer Operations	The Customer Operations role covers the activities related to the operation of the certified cloud service by the CSC within its own organization, possibly through another cloud service. The tasks involved depend on the cloud capabilities type, and may include configuration, deployment, and maintenance tasks, following the guidance provided with the certified cloud service.
Cloud Service Customer	Customer compliance	The Customer Compliance role covers the activities related to the verification of compliance of the CSC's own products or services, possibly includes other cloud services. In that context, the main aspects are the use of the evaluation performed on the cloud service and the reuse of evidence or conclusions generated during the cloud service evaluation.

Stakeholder	Role	Use case
Cloud Service User	User	The Cloud Service User is not expected here to be a primary user of the scheme, but they should be targeted as secondary users through Cloud Service Customers. Users are nevertheless directly targeted by some of the documentation provided by the CSP and evaluated in the context of the scheme, and their profile should be considered when developing and auditing user documentation.
Regulatory authority	Regulation	The Regulation role includes the development of rules and regulations to be applied at a local, regional, national or European level. Regulators may use the scheme as a basis for including high-level requirements (mandatory certification) or more detailed requirements, for instance building on transparency requirements.
Regulatory authority	Enforcement	The Enforcement role includes all activities related to the enforcement of regulations that mention the scheme. Enforcers will in particular need to verify that cloud service providers comply with the parts of the regulation that depend on the scheme.

Out of the stakeholders using the scheme, we can distinguish between primary users, including CSPs, CSCs and Regulatory Authorities, and secondary users, including CABs, NCCAs and Cloud Service Users. Among the secondary users, CABs and NCCAs are mentioned because they control the issuance of the certificates and NABs and ENISA are mentioned because they are directly involved in the operation of the scheme.

Cloud Service Users (the actual persons or machines using the certified cloud services) are not considered as primary users for two distinct reasons:

- Employees of a CSC are considered secondary users. The CSC as primary users select the cloud service and will provide its internal users with the recommendations provided by the CSP to securely use their services.
- Final customers are not considered as direct users of the scheme, because one of the prerequisites for being a user of the scheme is the ability to understand the information made available to CSCs, which requires some knowledge in cybersecurity that cannot be assumed from a final customer.

The intended users whose needs the scheme shall satisfy are the CSPs and the CSCs, as well as the Regulatory Authorities. Satisfying these needs is indeed the purpose of the scheme, with one distinct objective for each category of users:

- For CSPs. The scheme shall assess how a cloud service, as described by the CSP, meets the requirements of a predefined set of security control objectives and a related set of measures, when used according to security recommendations provided by the CSP.
- For CSCs. The scheme shall provide CSCs the information required to make informed choices about the procurement and operation of cloud services, and shall allow CSCs to use certified cloud services in their own development activities, and to meet their own security compliance requirements.
- For Regulatory Authorities. The scheme shall allow Regulatory Authorities to refer to the scheme in European and national regulations, including criteria based on information defined in the scheme, and it shall allow them to enforce regulations by verifying the information provided in the certificates stored in the site managed by ENISA

For CSPs, the scheme offers:

- a single certification scheme recognized across the entire European Union;
- three assurance levels corresponding to different needs from the CSPs and different use cases;
- two assessment methodologies tailored to the assurance levels, designed to simplify their integration with other established methodologies such as [ISO17021] or [ISAE3402];
- a set of objectives and requirements inspired from existing schemes and mapped to the assurance levels;
- the possibility to use composition to simplify the certification of cloud services that rely on other already certified cloud services; and
- a certificate that can be used to demonstrate that their cloud service fulfils the requirements of the scheme.

For CSCs, the scheme offers:

- a single certification scheme recognized the entire European Union;
- three assurance levels corresponding to different needs from the CSCs and different use cases;
- requirements mandating transparency about the split responsibility between the CSP and the CSC regarding security;
- requirements mandating transparency about the location of the processing and storage of data, and about the applicable laws; and
- the possibility to use composition to certify their own cloud service when needed.

For Regulatory Authorities, the scheme offers:

- a single certification scheme recognized the entire European Union;
- three assurance levels corresponding to different needs from the CSCs and different use cases; and
- requirements mandating transparency about the location of the processing and storage of data, and about the applicable laws.

4. USE OF STANDARDS

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following element

c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;



The scheme relies on a number of standards and technical specifications:

- International standards ISO/IEC 17788 and ISO/IEC 17000, and to a lesser extent ISO/IEC 9000 and ISO/IEC 27000, are being used as references for the terminology used through the scheme, with input from all the schemes listed below when required.
- The security controls used in the scheme, together with the associated security requirements, are defined in an Annex of the present scheme (see Annex A.: Security Objectives and requirements for Cloud Services), and they are based on international standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and on documents previously issued by Member States to define the security controls in their respective National Schemes [C5, SecNumCloud].
- The definition of the assurance levels reuses some concepts defined in the ISO/IEC 15408-3 standard.
- The conformity assessment methodology defined in the scheme is based on the ISO/IEC 17065 international standard.

The scheme also leverages several security assessment methods and standards:

- International standards ISO/IEC 17021 and ISO/IEC 27006.
- International auditing standards ISAE3402 and ISAE3000.
- One method defined in an Annex to the present scheme (see Annex D.: Assessment for level Basic).

The security controls and other annexes also reference a number of standards:

- The ISO/IEC 29147 and ISO/IEC 30111 standards are referenced about vulnerability handling
- The ISO/IEC27005 standard is referenced about risk management

RATIONALE

Additional input

This is reinforced in the request for the candidate scheme, which indicates that “the candidate scheme (...) should take into account existing and relevant schemes and standards.”

The text mentions regulation (EU) No 1025/2012, it defines the following requirements (this is an outline, further details are available in the regulation itself:

1. Market acceptance, as demonstrated by the existence of compliant implementations from different vendors
2. No conflict with current or foreseen European standard
3. Developed by a non-profit making organization which fulfils some criteria

- a) Openness of the specification development process
 - b) Consensus-based decision-making process
 - c) Transparency of the development process
4. Requirements on the specification itself
- a) Sustained maintenance for a long period
 - b) Publicly available for implementation and use on reasonable terms
 - c) IP rights essential to the specification are available on a (F)RAND basis
 - d) Relevant and effective, responding to market needs and regulatory requirements
 - e) Neutral and stable
 - f) Sufficient quality and level of details, with standardized interfaces available as needed

These requirements are classical, and they are based on the WTO rules, so they are in practice met by many of the technical specifications developed by all kinds of industry groups.

Regarding the elements included in the scheme itself, the following guidance has been provided to the SOGIS ad hoc working group:

- The elements that are mandatory for the implementation of the scheme must be included as appendices to the scheme, and they will be included in the regulation.
- The elements that are optional in the implementation of the scheme may be included in other documents, provided by ENISA on the certification framework portal.



The standards that are referenced are very classical in the IT security field.

However, in some cases, it has not been possible to rely solely on European and international standards.

For the security controls, the ISO/IEC 27000 series provides a very good basis, but it did not provide the level of details deemed suitable for the present scheme. The structure of the controls is strongly inspired from these standards, but the content has been enriched, in particular by introducing more detailed requirements that have been mapped to assurance levels. These requirements have been designed by drawing inspiration from current practices in Europe, and in particular from the documents issued by Member States who operated National Schemes for cloud services.

For the assessment methods, the scheme recognizes the two most widely used assessment method families (based on the ISO/IEC 17000 family and on the ISAE3000 family), but there has been a need to add a specific and simplified assessment method for the 'basic' level, which is defined in the scheme itself.

Both documents have been written in a way that could allow them to be considered as a basis for the establishment of new standards.

5. ASSURANCE LEVELS

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(d) where applicable, one or more assurance levels;



The scheme defines three assurance levels, with assurance level Basic corresponding to the 'basic' assurance level of the EUCSA, assurance level Substantial corresponding to the 'substantial' assurance level of the EUCSA, and assurance level High corresponding to the 'high' assurance level of the EUCSA.

As specified in the EUCSA's Article 52(5), assurance level Basic is "intended to minimise the known basic risks of incidents and cyberattacks" and can be further defined as follows:

- Assurance level Basic should provide limited assurance that the cloud service is built and operated with procedures and mechanisms to meet the corresponding security requirements at a level intended to minimize the known basic risks of incidents and cyberattacks.
- Assurance level Basic should be suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems.
- The typical attacker profile for assurance level Basic should be a single person with limited skills repeating a known attack with limited resources, not including the ability to perform social engineering attacks.
- The evaluation scope for assurance level Basic shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to assurance level Basic, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including processes and the software (understood as result of a development process) underlying the service.
- The evaluation depth for assurance level Basic shall consist solely of inspection activities, based on a check for completeness and coherence of the provided documentation on processes and design intended to confirm the fulfilment of technical and organizational measures, including requirements for fully automated testing of basic known vulnerabilities and automated compliance checks by the CSP.
A report following defined procedures shall be generated by the CAB.
Self-gathered evidence shall be regularly submitted to the CAB to justify the continued development and operation of the service.
- The evaluation depth for assurance level Basic shall be driven by a predefined audit plan.

As specified in the EUCSA's Article 52(6), assurance level Substantial is "intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources" and can be further defined as follows:

- Assurance level Substantial should provide reasonable assurance through evaluation by a CAB that the cloud service is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The CAB shall determine that the cloud service provider has assessed those risks and implemented suitable controls that, if operating effectively, minimize those risks and meet the corresponding security requirements throughout a specified period.
- Assurance level Substantial should be suitable for cloud services that are designed to meet typical security requirements on services for business-critical data and systems.

- The typical attacker profile for assurance level Substantial should be a small team of persons with hacking abilities and access to a wide range of known hacking techniques, including social engineering, but with limited resources, in particular to launch wide attacks or to discover previously unknown vulnerabilities.
- The evaluation scope for assurance level Substantial shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to assurance level Substantial, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including processes and the software (understood as result of a development process) underlying the service. The effective operation of the relevant security controls shall also be demonstrated throughout a specified period.
- The evaluation scope for assurance level Substantial shall include, in addition to the requirements for assurance level Basic, on-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design, including the validation of the functional tests performed on that implementation.

The security controls for assurance level Substantial shall include a limited pen testing using known attacks.

As specified in the EUCSA's Article 52(7), assurance level High is "intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources" and can be further defined as follows:

- Assurance level High should provide reasonable assurance through evaluation by a CAB that the cloud service is built and operated with procedures and mechanisms to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The CAB shall determine that the cloud service provider has assessed those risks and implemented suitable controls that operated effectively to minimize those risks and meet the corresponding security requirements throughout a specified period.
- Dedicated requirements are defined in Annex A: (Security Objectives and requirements for Cloud Services) to ensure that controls shall be automatically monitored for continuous operation in accordance with their design, and that the controls shall be regularly reviewed and pen tested to validate their actual ability to prevent or detect security breaches.
- Assurance level High should be suitable for cloud services that are designed to meet specific (exceeding level 'substantial') security requirements for mission-critical data and systems.
- The typical attacker profile for assurance level High should be a team of highly skilled persons with access to significant resources to design and perform attacks, get insider access, discover or buy access to previously unknown vulnerabilities.
- The evaluation scope for assurance level High shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to assurance level High, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including processes and the software (understood as result of a development process) underlying the service. The effective operation of the relevant security controls shall also be demonstrated throughout a specified period.
- The evaluation depth for assurance level High shall be based on the depth for assurance level Substantial, to which requirements on depth of inspection or testing shall be added to verify that the controls implemented by the CSP actually meet their objective.

In particular, these requirements concern the automated monitoring of controls and the review and penetration testing of security controls. Such activities shall be planned over multiple years, and they shall be performed by personnel with appropriate competences, in particular when penetration testing or in-depth technical reviews are required.

- The evaluation depth for assurance level High shall be driven by a full justification of the coverage for all mappings, including for processes.

It may also include higher expectations for some processes and their implementation, as defined in the security controls pertaining to assurance level High.

RATIONALE

Additional input

Article 52 provides details about the assurance levels, and in particular:

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT processes: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service or ICT process, in terms of the probability and impact of an incident.
3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.
5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level 'basic' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
6. A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.
7. A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.

Recitals also provide additional information about assurance levels

(65) The assurance level of a European certification scheme is a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure the consistency of the European cybersecurity certification framework, a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each European cybersecurity certificate might refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity might only refer to the assurance level 'basic'. The assurance levels would provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.

(66) A European cybersecurity certification scheme might specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Evaluation levels should correspond to one of the

assurance levels and should be associated with an appropriate combination of assurance components. For all assurance levels, the ICT product, ICT service or ICT process should contain a number of secure functions, as specified by the scheme, which may include: a secure out-of-the-box configuration, a signed code, secure update and exploit mitigations and full stack or heap memory protections. Those functions should have been developed, and be maintained, using security-focused development approaches and associated tools to ensure that effective software and hardware mechanisms are reliably incorporated.

(67) For assurance level 'basic', the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentation of the ICT product, ICT service or ICT process by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review. Where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes has carried out a self-assessment of the compliance of the ICT product, ICT service or ICT process with the certification scheme.

(68) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

(69) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.



High-level presentation

All Assurance level defined in the EUCS scheme satisfy all requirements that are applicable to all EUCSA assurance levels:

- Every assurance level is commensurate with the level of risk associated to the intended use of the cloud service, as demonstrated in the definition of suitable services and typical attacker profiles (Article 52(1)).
- Every assurance level defines security requirements and functionalities, as well as the rigour and depth required in the evaluation (Article 52(3)).
- Every assurance level requires that evaluation activities include a review of technical documentation (Article 52(5), Recital 67).
- Every assurance level requires a review of the cloud service's main processes, including the development process used for the development of the cloud service (Recital 67).

Those are the only requirements defined for assurance level 'basic' in the EUCSA, which are all satisfied by assurance level Basic.

In addition, assurance level Substantial satisfies the requirements pertaining to the EUCSA's assurance level 'substantial':

- Assurance level Substantial security controls include a vulnerability assessment activity that perform a review of publicly known vulnerabilities (Article 52(6)).
- Assurance level Substantial security controls include a review of the functional tests of the cloud service's security functionalities as well as some independent testing requirements (Article 52(6)),
- The assessment methodology for assurance level Substantial mandates the review of a mapping between the documentation of security functionalities and their implementation to ensure compliance (Recital 68).

Finally, assurance level High satisfies the requirements pertaining to the EUCSA's assurance level 'high':

- Assurance level High security controls include a vulnerability assessment activity that perform a review of publicly known vulnerabilities (Article 52(7)).
- Assurance level High security controls include a review of the functional tests of the cloud service's security functionalities, as well as automated monitoring requirements, (Article 52(7)),
- Assurance level High security controls require the use of state-of-the-art security functionalities (Article 52(7)).
- The assessment methodology for assurance level High mandates the review of a full mapping between the documentation of security functionalities and their implementation to ensure compliance (Recital 68).
- The assessment methodology for assurance level High mandates both design efficiency and operating efficiency to be assessed during the evaluation (Recital 69). This assessment includes penetration testing to assess the resistance of security functionalities of the cloud services (Article 52(7), Recital 69).

Note that, throughout this document, references to the assurance levels defined in the EUCSA use lowercase and quotes ('basic', 'substantial', 'high'), whereas the assurance levels defined in EUCS are capitalized (Basic, Substantial, High). The names assigned to assurance levels in EUCS may be later modified.

DETAILED PRESENTATION

This presentation is the full output of the thematic group on assurance levels, which provides a full background

PARAMETERS

Intention

The intention provides a general description of the Assurance Level, most likely matching quite closely the definition from the EU CSA.

Suitability

Suitability is about potential restrictions of the types and categories that may be covered.

Attacker profile

The attacker profile cannot be very specific, because of the great variety of attackers, and it always defines a wide category of attackers. Typical expected results are as follows:

- The least sophisticated attackers in the range should be stopped, regardless of their motivation.
- The most sophisticated attackers in the range should be deterred to attack that particular service. This means that, if they have a specific reason to attack that particular service, they may succeed with difficulties, but if they are looking for generic revenue, the difficulty should encourage them to move to the next target.

Note that this applies as well to the 'high' level. Security certification cannot provide guarantees against a motivated nation-state determined to attack a specific site but may discourage them if they are "harvesting" information.

Scope of the Evaluation

In ISO/IEC 15408-3, scope is defined as "*the effort is greater because a larger portion of the IT product is included*". This is about gradually adding elements to be evaluated. The scope of the evaluation should comprise the service provided by the CSP and clearly identify all underlying and supporting services and processes.

Depth

In ISO/IEC 15408-3, depth is defined as "*the effort is greater because it is deployed to a finer level of design and implementation detail*". This is about considering more and more details and asking more precise questions. The general principle is to follow an incremental approach, *i.e.*, that all requirements of a lower level are similarly included in the depth of the higher level.

Rigour

In ISO/IEC 15408-3, a more rigorous assessment is defined as "*the effort is greater because it is applied in a more structured, formal manner*". This is about requiring more structure in the service (for instance, a security model based

on a specific formalism/method) or adding more structure to the assessment (for instance, requiring a specific method to collect evidence or provide results).

APPLICATION TO ASSURANCE LEVELS

Level	Basic	Substantial	High
Intention	Provide limited assurance through a review by an independent third party that the cloud service is built and operated with procedures and mechanisms to meet the corresponding security requirements at a level intended to minimize the known basic risks of incidents and cyberattacks.	Provide reasonable assurance through evaluation by an independent third party that the cloud service is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The CSP has assessed those risks and implemented suitable controls that, if operating effectively, minimize those risks and meet the corresponding security requirements throughout a specified period.	Provide reasonable assurance through evaluation by an independent auditor that the cloud service is built and operated with procedures and mechanisms to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The CSP has assessed those risks and implemented suitable controls that operated effectively to minimize those risks and meet the corresponding security requirements throughout a specified period. Security controls are monitored for continuous operation in accordance with their design; they are reviewed and pen tested to validate their actual ability to prevent or detect security breaches.
Intention rationale	Scope, depth and rigour of the assurance level is limited to procedures and mechanisms for those security requirements that shall minimize basis risks only.	Scope, depth and rigour of this assurance level requires the cloud service provider to apply a risk-based approach for the suitable design and implementation of controls that meet the corresponding security requirements. The systematic risk assessment approach and the operating effectiveness (consistent application) of controls throughout a specified period is evaluated by an independent auditor, including for the initial conformity assessment.	Scope, depth and rigour of this assurance level extend the previous level for Substantial by additional procedures to be performed for automated controls. Automated monitoring is applied by the CSP to identify exceptions in the application of controls (e.g. changes to the configuration) and initiate corrective actions. Reviews and pen tests are performed by the independent auditor or a third party engaged by the CSP with the objective to identify vulnerabilities that allow to circumvent, override or breach controls.
Suitability	The Basic level is suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems.	The Substantial level is suitable for cloud services that are designed to meet typical security requirements on services for business-critical data and systems.	The High level is suitable for cloud services that are designed to meet specific (exceeding level 'substantial') security requirements for mission critical data and systems.

Level	Basic	Substantial	High
Suitability rationale	The 'Basic level provides limited assurance that baseline procedures and mechanisms are in place to address security risks and threats in potentially low impact information systems (e.g.: Web site hosting public information). It is typically not suited for Platform or Infrastructure capabilities, used by a large number of services. built on top and that require an elevated level of security. The Basic level demonstrates a willingness to address security, including the application of security guidance from subservice providers.	The Substantial level provides reasonable assurance that a set of more stringent (than in level Basic) security controls is designed and operated to address security risks and threats in potentially moderate impact information systems to protect business critical information (e.g.: Confidential business data, email, CRM – customer relation management systems, personal information). It is suitable for all capabilities types. . The Substantial level demonstrates a robust and mature holistic security management to provide secure services.	The High level provides reasonable assurance that a set of even more stringent security controls is designed and operated to address security risks and threats in potentially high impact information systems to protect mission critical information (e.g. highly confidential business data, patents). The costly and rigorous evaluation process reflects the intention to minimize the risks in using the cloud service.
Attacker profile	Single person with limited skills repeating a known attack with limited resources, not including the ability to perform social engineering attacks.	Small team of persons with hacking abilities and access to a wide range of known hacking techniques, including social engineering, but with limited resources, in particular to launch wide attacks or to discover previously unknown vulnerabilities.	Team of highly skilled persons with access to significant resources to design and perform attacks, get insider attacks, discover or buy access to previously unknown vulnerabilities.
Attacker profile rationale	Today, Basic is about removing low-lying fruits and ensuring that cloud services, including simple ones, are designed with security in mind. The objective is to remove the possibility to fall victim to trivial attacks. When such certification becomes mainstream, the requirements should be revised upwards.	This is the “standard” attacker, corresponding to most real-life attacks used to disclose information, steal resources, deny service, or tamper with a service. Their main characteristics come from the definition of the level: “known attacks” and “limited resources”. Note that this definition is quite ambitious and allows the use of attacks that leverage several vulnerabilities.	This is the sophisticated attacker, against which detection and mitigation is more efficient than resistance. At this level, it may be difficult to define precisely a way to analyse that the objective has been met, in particular because there is an expectation to minimize risks through various mitigation methods.
Scope	As defined by the service description and the controls pertaining to the Basic level, including processes and the software (understood as result of a development process) underlying the service.	As defined by the service description and the controls pertaining to the Substantial level, including processes and the software (understood as result of a development process) underlying the service. Operating effectiveness of the controls shall be demonstrated.	As defined by the service description and the controls pertaining to the High level, including processes and the software (understood as result of a development process) underlying the service. Operating effectiveness of the controls shall be demonstrated. (including automated monitoring if required by the control definition).
Scope rationale	This may need to be rephrased, depending on the relationship between “controls” and “requirements”. Here, the idea would be to include all controls in their general form, but without the more detailed requirements that may be added for higher levels.	We refer to the same controls from the Basic assurance level, but with the stronger refinements or enhancements (e.g., (mandated techniques, thresholds, etc). Requirements must include a limited pen testing using known attacks.	We refer to the same controls from the Substantial assurance level, but with the higher refinements or enhancements. Enhancements often included additional constraints, references to state-of-the-art requirements, and automated monitoring of some controls.

Level	Basic	Substantial	High
Depth	<p>Inspection solely, based on a check for completeness and coherence of the provided documentation on processes and design intended to confirm the fulfilment of technical and organizational measures, and interactions between the auditor and the CSP at the beginning and at the conclusion of the inspection.</p> <p>A report following defined procedures is generated by the inspection body.</p> <p>Once a year, a documentation update is provided for third-party review of the continued development and operation of the service.</p>	<p>Additional to the requirements of Basic: On-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified policies and procedures, and an additional focus on development activities, for instance on the functional tests performed.</p> <p>On the initial assessment and once a year, the operating effectiveness of the security controls, <i>i.e.</i> their operation as designed, needs to be demonstrated over the previous period.</p>	<p>Additional to the requirements of Substantial: Specific requirements on the monitoring and testing of the controls, <i>i.e.</i> their operation as intended to protect from attacks or detect them, needs to be demonstrated.</p> <p>Different measures may be used, such as technical reviews, and penetration testing shall be performed by qualified personnel, following a multi-year plan that needs to be validated in the audit.</p>
Depth rationale	<p>The inspection focuses on completeness, coherence and plausibility of the documentation. It needs to be an efficient process that mostly focuses on the existence of processes, and of a secure by design approach, to demonstrate the proper design and existence of security measures to protect the cloud service.</p>	<p>The full audit aims at providing reasonable assurance that the security controls are properly designed and operate effectively, <i>i.e.</i> as designed, over a period of time.</p>	<p>The audit aims at providing the same reasonable assurance as for the Substantial level.</p> <p>The main addition in depth come from additional requirements for level High, such as automated monitoring and penetration testing, which are intended to demonstrate that the controls remain effective under strenuous conditions.</p>
Rigour	<p>The assessment is performed by the CSP and driven by a standardised checklist.</p> <p>An accredited third-party then audits the assessment report and its supporting documentation.</p>	<p>The assessment is performed by an accredited third-party, and it is driven by a risk analysis performed by the CSP, which is in the audit scope.</p>	<p>The assessment is performed as for the Substantial level, but the CAB needs to be authorized by the NCCA to it has the required competencies to audit the specific requirements of the High level.</p> <p>More rigour is expected in the definition and application of policies, usually as defined in requirements specific to the controls (<i>e.g.</i> the need to demonstrate the coverage of functional tests used in development).</p>
Rigour rationale	<p>The assessment follows all items in a checklist suited to the targeted cloud service, and its results are reviewed by an accredited third-party.</p>	<p>A full audit is performed by an independent third-party, and the checklist approach is replaced by a more rigorous risk-based approach, allowing the auditor to identify controls that require specific attention.</p>	<p>The rigour remains mostly the same as for level Substantial, as it corresponds to typical audit conditions.</p> <p>Nevertheless, specific requirements explicitly increase the level of rigour on some controls by requiring additional deliverables from the CSP.</p>

6. SELF-ASSESSMENT

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (e) an indication of whether conformity self-assessment is permitted under the scheme;



EU statements of conformity shall not be issued by CSPs in the EUCS scheme.

RATIONALE

Additional input

In addition, Article 53, provides further information on conformity self-assessment, and in particular:

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.
2. The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services or ICT processes shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in that scheme.

Recitals also provide additional information:

(78) European cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all of the checks to ensure that the ICT products, ICT services or ICT processes conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms. Moreover, conformity self-assessment should be permitted for ICT products, ICT services or ICT processes only where they correspond to assurance level 'basic'.

(79) European cybersecurity certification schemes could allow for both conformity self-assessments and certifications of ICT products, ICT services or ICT processes. In such a case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between ICT products, ICT services or ICT processes with regard to which the manufacturer or provider of ICT products, ICT services or ICT processes is responsible for the assessment, and ICT products, ICT services or ICT processes that are certified by a third party.



The issuance of EU statements of conformity by cloud service providers could only have been allowed for all cloud services that present a low risk (Article 53(1)), *i.e.*, to a subset of the cloud services that could be certified at level Basic.

The ad hoc Working Group consistently expressed that self-assessment was not suitable for cloud services, even at level Basic and even on a strictly defined subset of services. In addition, there are many elements in the scheme, including the definition of the security objectives and requirements, that are entirely new. Rather than allowing CSPs to interpret these security requirements, it is preferable to only allow accredited CABs to use the scheme, making it easier to bring the various elements of the scheme to a higher level of maturity in a consistent way, and to control their usage in the meantime through guidance and guidelines for CABs.

Although divergent opinions have been expressed, in particular in the surveys performed over the summer, we have decided to not allow the issuance of EU statements of conformity in the initial version of this scheme, as there are enough challenges to be met in that first version.

This decision may be reconsidered in future releases of the scheme.

7. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;



All CABs performing assessments in the context of the EUCS scheme will need to be accredited for [ISO17065], complemented by the requirements defined for the EUCS scheme (see Annex E: Competence requirements for CABs). The requirements will define several profiles corresponding to the various roles in the conformity assessments, in order to allow CABs that only perform a subset of the of the conformity assessment activities, in particular those that only perform evaluation activities.

The technical competence requirements associated to accreditation are sufficient to perform conformity assessments at levels Basic and Substantial. However, advanced competences are required in order to perform a conformity assessment at level High. As a consequence, conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out in the context of an evaluation at level High conformity assessment tasks related to highly technical topics including:

- Penetration testing, including the design and performance of penetration tests and the analysis of penetration testing activities performed by a CSP or its contractors.
- Analysis of development activities, and in particular the review of the design and implementation of security measures by the CSP.

Further details are provided in Annex E: (Competence requirements for CABs).



RATIONALE

Additional information from the EUCSA

Article 60 covers Conformity assessment bodies:

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.

3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

Article 58, about National Cybersecurity Certification Authorities, also covers that topic:

7. National cybersecurity certification authorities shall:

(c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;

(e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation;

The Annex to the Cybersecurity Act (Requirements to be met by Conformity Assessment Bodies) provides detailed information on the conditions to be met by all CABs. However, it does not include any reference to point (f) of Article 54 (1), so we don't reproduce it here.



The competence required for CABs are rather generic, since most of the controls are related to the processes used by the CSP. Nevertheless, some controls require competences, in particular at the highest levels of assurance.

Pen testing and analysis of development activities are provided as examples, since those activities do require specific competencies, but the “including” formulation does not preclude the addition of further activities.



8. EVALUATION METHODS AND CRITERIA

Foreword for Reviewers

The present chapter is not fully ready for review, the evaluation methods and criteria are still being defined. The structure is set, though, and we are mostly missing the mapping between the measures in the scheme and the security objectives of Article 51.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;



The EUCS scheme uses a set of evaluation criteria that is defined in Annex A: (Security Objectives and requirements for Cloud Services).

The EUCS assessment methodology, based on the [ISO17065] standard, is defined in Annex B: (Meta-approach for the assessment of cloud services). This methodology defines two assessment approaches that may be used by CABs:

- an assessment approach that may be used for assurance levels Substantial and High, defined in Annex C: (Assessment for levels Substantial and High), which draws inspiration from both the [ISO17021] standard and from the ISAE family of standards [IAASB Handbook];
- an evidence-based assessment approach, defined in Annex D: (Assessment for level Basic), that may be used solely for assurance level Basic.

In order to achieve a high level of interoperability between the assessment methods, the EUCS assessment methodology also defines strict guidelines and requirements on the assessment process and on its deliverables, which shall be followed independently of the assessment method used in a specific evaluation.

Article 51 objectives are covered by the security objectives requirements defined in Annex A: (Security Objectives and requirements for Cloud Services). Table 3 below provides a high-level vision based of the coverage of Article 51 requirements by security categories from Annex A:.

Table 3: Coverage of Article 51 by requirement categories

Security objectives from Article 51	Categories from Annex A:
(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;	This is covered in many categories of the scheme, including in particular the CKM category (covering cryptography) and the CS category (covering the security of communications)
(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;	This is covered in many categories of the scheme, including in particular the CKM category (covering cryptography) and the CS category (covering the security of communications)
(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	This is mostly covered by the IAM category (covering identity management, authentication, and access control)
(d) to identify and document known dependencies and vulnerabilities;	This is mostly covered by the PM category (defining relationships with suppliers) and the OPS category (defining vulnerability handling)
(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	This is mostly covered by the OPS category (defining logging)
(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	This is mostly covered by the OPS category (defining logging)
(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	This is mostly covered by the OPS category (defining general pen testing measures) and by the DEV category (defining vulnerability testing in the development context)
(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	This is mostly covered by the BCM category (defining business continuity) and the PS category (defining physical security measures)
(i) that ICT products, ICT services and ICT processes are secure by default and by design;	This is mostly covered in the DEV category (defining methodology), with complements in many other categories
(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	This is mostly covered by the OPS category (vulnerability handling), in the CCM category (for change management) and in the DEV category (for development methodologies)

RATIONALE

Additional information from the EUCSA

Article 51. Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be designed to achieve, as applicable, at least the following security objectives:

- (a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;
- (b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process;

- (c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;
- (d) to identify and document known dependencies and vulnerabilities;
- (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;
- (g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;
- (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;
- (i) that ICT products, ICT services and ICT processes are secure by default and by design;
- (j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

Recital (74) provide a rationale for Article 51:

(74) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT processes should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications if no appropriate standards are available.



The requirements defined in the EUCS scheme have been drawn from a number of existing standards and conformity assessment schemes, and they cover all categories defined in information security standards such as [ISO27001]. In particular, the structure of the requirements is inspired from the [C5] criteria and from the [SecNumCloud] scheme.

Regarding assessment methods, a key objective from the scheme has been to minimize the disruption of existing practices regarding certification and assurance for CSPs. The choice was made to use a hybrid methodology, based on both the [ISO17021] methodology that is used for [ISO27001] certifications and on the [ISAE3402] methodology used by many companies to get assurance reports on the security of their information systems.

As a result, the proposed methodology presents numerous advantages:

- It proposes several assurance levels with increasing requirements that correspond to the levels defined in [EUCSA];
- It allows combined assessments with both [ISO17021] and [ISAE3402] assessments, allowing CSPs to contain the investment on compliance.



9. NECESSARY INFORMATION FOR CERTIFICATION

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;



When a CSP wishes to get a cloud service certified in the EUCS scheme, or to maintain the certification of an already certified cloud service, the CSP shall submit an application document, following the template defined in Annex F: (Scheme Document Content requirements), completed with all required information, which depends in part on the reason that triggered the conformity assessment.

During the evaluation, the CSP shall submit all the information needed to demonstrate that the implementation of their cloud service meets the security requirements defined in Annex A: (Security Objectives and requirements for Cloud Services) for the targeted assurance level, including but not limited to:

- policies and procedures defined at the organization level and that apply to the design and operation of the cloud services under evaluation;
- policies and procedures that are specific to the design and operation of the cloud services under evaluation;
- documentation related to the cloud services under evaluation, including design documentation, and if required, test documentation, implementation details;
- if required, records that can be used as evidence that the abovementioned policies and procedures are being followed;
- if subservice organizations are used, records and documents that can provide assurance that the subservice organizations satisfy the requirements of the scheme that they are responsible for;
- where explicitly stated, specific documents and records required by the CAB to assess the fulfilment of requirements pertaining to specific security controls.

The information to be provided also depends on the assurance level required for the certification, as defined in Chapter 5 (Assurance Levels). The information shall be provided following the assessment processes defined in Annex B: (Meta-approach for the assessment of cloud services), Annex C: (Assessment for levels Substantial and High) and Annex D: (Assessment for level Basic).

In the context of the conformity assessment, the CSP shall grant the CAB:

- access to all information, such as records and documentation, including service level agreements, of which management is aware that is relevant to the cloud service;
- access to additional information that the CAB may request from management for the purpose of the evaluation;
- unrestricted access to personnel within the Service Organization from whom the CAB determines it may be necessary to obtain evidence relevant to the evaluation;

All records and documentation supporting the conformity assessment shall be appropriately archived by the CSP and/or the CAB, as defined in Chapter 15 (Record Retention) and Chapter 18 (Availability of Information).



As part of a new certification, it shall be possible to reuse evaluation results from another ICT certification or assessment. The applicant may therefore make available to the CAB previous evaluation results to be re-used as evidence. The CAB shall reuse such results for its tasks only when the provided evidence conforms to the requirements for such evidence, the evidence has been evaluated following a methodology recognized by the scheme, and the authenticity of the evidence can be confirmed.

In addition, the CSP shall submit to the CAB the link to the supplementary cybersecurity information required by Article 55 of the EUCSA, in accordance to the rules defined in Chapter 23 (Supplementary Information).

Security requirements are defined in Annex A: (Security Objectives and requirements for Cloud Services) related to the availability and content of this supplementary information, to be fulfilled by certified cloud services at all assurance levels

Additional information may be required when the conformity assessment is performed as a consequence of the vulnerability management process defined in Chapter 14 (New Vulnerabilities), or of the nonconformity management process defined in Chapter 13 (Non-Compliance), to ensure that the vulnerability or nonconformity has been properly handled.

An important part of the information provided by the CSP is the description of its cloud service, which shall follow the principles below:

- The description shall provide the information that is likely to be relevant from a CAB's perspective to understand the cloud service and associated controls to meet the applicable EUCS requirements as defined in Annex A: (Security Objectives and requirements for Cloud Services). Other aspects of the cloud service do not need to be covered in the provided information.
- If the CSP uses subservice organizations in the provision of the cloud service, the description shall indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the CSP's own controls, to meet certain of the EUCS requirements. The information shall include a presentation of applicable EUCS requirements, with the CSP's controls, the types of complementary subservice organization controls assumed in the design of the CSP's controls, and pointers to assurance documentation where evidence can be found that the subservice organization satisfies these complementary subservice organization controls with an level assurance suitable for the targeted level of assurance. The assurance documentation referred to in that presentation shall be included in the information provided to the CAB.
- The description shall indicate that Complementary Customer Controls that are suitably designed and are operating effectively are necessary, along with the CSP's controls, to meet some of the applicable EUCS requirements. The description shall present the applicable EUCS requirements, the CSP's controls and the Complementary Customer Controls assumed in the design of the CSP's controls.

General rules regarding the protection of the information provided by an applicant shall comply with the requirements established under Chapter 24 (Additional Topics).

RATIONALE

The information to be provided by the CSP is mostly guided by the requirements defined in the security controls in Annex A: (Security Objectives and requirements for Cloud Services). The present chapter only defines the main principles, which grants the CAB both necessary and limited access to:

- all pertinent documents, including policies and procedures, as well as records, logs, and other documents that can attest that the procedures and policies are being applied appropriately;
- interactions with employees, including individual interviews and group meetings, to gather information on the application of procedures, or to provide explanations pertaining to the definition and implementation of security controls;
- interactions with the CSP systems, in particular to verify that technical security controls are properly implemented, which may either be performed directly by an auditor, or performed by a CSP employee in front of an auditor.

There may be some restrictions in the availability of the information, in particular related to the confidential nature of the information, so some information may only be available to the CAB for a limited time, and only on the premises of the CSP. Such limitations should be considered in the contractual agreement between the CAB and the CSP, to ensure that they are acceptable to the CAB and that possible additional costs are covered by the CSP.

In addition to the information related to the requirements, the CSP needs to provide other information to the CAB for evaluation:

- the supplementary cybersecurity information required by Article 55 of the EUCSA;
- any relevant information pertaining to a vulnerability or nonconformity that has triggered the conformity assessment.

This provision has been added in the case where the CAB would need specific information related to an issue or to the supplementary cybersecurity information that has not been explicitly planned in the security controls' requirements.

10. MARKS AND LABELS

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;



The European Cybersecurity Certification Framework may provide for a label and associated mark.

When available, such a label shall be specifically implemented for this scheme, in order to allow its application on each certificate, certified cloud service and related documentation. The labels used on the cloud service and related documentation shall contain exactly the same information as the label included on the certificate, and follow all the guidelines provided with the label and associated mark defined for the European Cybersecurity Certification Framework.

A label and associated mark shall only be used when the certificate is awarded and until its expiration, and in association with the certified cloud service: the non-respect of this condition shall be considered as an irregularity, as defined by Chapter 11 (Compliance Monitoring).



Without prejudice to the rules for monitoring compliance as described under Chapter 11 (Compliance Monitoring), depending on the circumstances, the nature and impact of the non-respect, wrong use, misuse, abuse of the mark and or label may have other legal implications in the field of IP right protection, possible criminal allegations (e.g. fraud, deceit), market surveillance regulations related to consumer protection (e.g. misleading and or unlawful comparative advertising of cloud services). These legal implications are outside the scope of this EUCS scheme.

RATIONALE

A label and associated mark, established for the European Cybersecurity Certification Framework and specifically implemented for this scheme, will allow to:

- highlight that the cloud service has been certified in the European Union and to provide immediate information regarding the certificate by referring to the framework (ECCF), the evaluation scheme and the assurance level;
- make the certification easily recognizable as both the label and the associated mark may be used in the cloud service’s web site and printed on technical documents and on leaflets used for marketing purposes;
- provide a direct link (in the form of a QR code) to the ENISA website (as per Article 50) - where all the information regarding the certificate are disclosed, including the current status of the certificate.

Figure 1: Demo label for the EUCS scheme

ECCF LOGO*	EUCS LOGO*
Certified in the European Union 	ECCF ENISA website 
CSA – Assurance Level (basic / substantial / high)	EUCS-specific Assurance Level name

* Logo and rules for its usage to be developed by the entity that registers the respective logo.

The “demo label”, shows the basic information that the label associated with the scheme may contain:

- logo of the ECCF (to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework);
- logo of the EUCS (to be registered, regulated and protected by the entity in charge of the enforcement of the labelling framework);
- QR code pointing to the web portal of ENISA - as per the Article 50 of the CSA – and to the page where the effective status of the certificate of the cloud service and the information regarding its lifecycle can be retrieved;
- CSA assurance level (with the introduction of a specific colour identifying each level);
- specific EUCS assurance level;
- the sentence “Certified in the European Union”, together with the flag of the EU.

The introduction of the QR code will imply, as defined by Chapter 20 (Disclosure Policy), a procedure for the release of the QR code.

The demo label only contains summary information. In particular, it does not contain any reference to a date or to an issuing CAB. The use of the label therefore needs to be strictly controlled to ensure that:

- The label is only used in direct relationship with a certified cloud service;
- The label is only used when the corresponding certificate is valid (i.e. after issuance, before withdrawal or expiration);
- The assurance levels and logos mentioned on the label are the appropriate ones for the particular cloud service; and
- The label is only used with the QR-code obtained through the procedure defined in Chapter 20, which points to ENISA’s Web site.

Compliance monitoring is in charge of ensuring that CSPs comply to these requirements.

11. COMPLIANCE MONITORING

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;



Without prejudice to NCCA activities defined under Articles 58.7 and 58.8 of the EUCSA, monitoring compliance of cloud services that have been issued European cybersecurity certificates shall demonstrate their continued compliance with the specified cybersecurity requirements.

In particular, this monitoring shall allow where possible to avoid and where needed to detect the following general cases of non-compliance:

- a non-compliance in the application by a CSP of the rules and obligations related to a certificate issued on their cloud services;
- a non-compliance in the conditions under which the certification takes place and that are not related to the individual cloud service;
- a nonconformity of a certified cloud service with the EUCS security requirements, which includes and is not limited to:
 - a change in the cloud service itself leading to a change of the cloud service's security posture;
 - a significant security incident that has affected the certified cloud service or has resulted in a data breach or loss of sensitive information;
 - a change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified cloud service;
 - a vulnerability identified and related to the certified cloud service, that has an adverse impact on the security of the certified cloud service.

The general monitoring of the certified cloud services shall be based on sampling, using generic criteria such as cloud service capabilities, assurance level, CSP, CAB and any relevant information brought to the knowledge of the NCCA (e.g., complaints, security events). The NCCAs on their respective territories and in cooperation with other relevant market surveillance authorities, shall sample annually a minimum of 5% of the cloud services which have been the subject of a successful conformity assessment in the context of the EUCS scheme in the previous year and at least one cloud service per annum.

The NCCA shall involve in the monitoring the CAB that has issued the certificate, and if necessary, its subcontractors. The monitoring shall consist in the re-assessment of the cloud service, together – when necessary – with an audit to confirm or disprove the above-mentioned relevant information brought to the knowledge of the NCCA. The re-assessments and audits procedures are defined in Annex G: (Certification Lifecycle and continued assurance).

Where a cloud service is selected the CSP shall be informed of the selection reasons.

Re-assessments and audits shall be financially supported by the CSP.

In addition to this general monitoring, the activities described hereinafter shall be undertaken.

The following deviations and irregularities shall be considered as potential non-compliance elements in the application by a CSP of the rules and obligations related to a certificate issued on their cloud service:

- any deviation from the requirements applicable to the information supplied or made available to a CAB, and that might be discovered after the emission of a certificate, such as:
 - a version of the information delivered that does not correspond to the version of the cloud service when it was certified;
 - self-established evidence that was not in-line with the reality of the cloud service;
- any deviation from the requirements regarding the certificate content and the supplementary information as required by Chapter 9 (Necessary information for certification), Chapter 17 (Certificate Format), Chapter 18 (Availability of Information), and Chapter 23 (Supplementary Information), including and not limited to:
 - deviation from referencing the proper cloud service identifiers;
 - misalignment of the description of the cloud service scope³;
 - deviation from constraints of the certificate including those of Chapter 12 (Certificate Management)⁴;
 - deviations from the conditions of use of the scheme's marks and labels as defined in Chapter 10 (Marks and Labels);
 - undue modifications or alterations of the certificate document as defined in Chapter 17 (Certificate Format);
 - omission to declare alteration of supplementary information as defined by Chapter 18 (Availability of Information);
- any deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity, such as:
 - failure to apply mandatory maintenance activities;
 - failure to implement and enforce mandatory processes as requested by the Terms and Conditions of a certificate and of the label;
 - deviations from the certified cloud service scope, including obligations from Article 56.8 of the EUCSA, including: undeclared modifications of the cloud service, its development and operating processes, the list of its dependencies⁵, or the list of utilized tools⁶.

Such non-compliance in the application by a CSP of the requirements related to a certificate issued on their cloud service shall be monitored by:

1. requiring any applicant to a certificate to commit to the CAB to a number of obligations, including but not limited to:
 - to transmit information to the CAB deemed reliable and that would not risk falsifying their judgment;
 - not to declare a cloud service as certified while the evaluation is still undergoing;
 - to declare a cloud service as certified only for the scope specified in the certificate;
 - to stop immediately the use of any advertisement mentioning the certification in the event of suspension or withdrawal of the certification;
 - to make sure that the cloud service operated with references to the issued certificate is the one which was the object of certification⁷;
 - to commit to scrupulously respecting the rules of use of the label established for the scheme; and
 - to notify the CAB about significant changes in the certified cloud service, including but limited to changes of subservice organizations, changes in the supplementary information or in any documentation element that is provided with the certificate.
2. using the following available dispositive to track the non-respect of the previous obligations:
 - the activities of market surveillance established under Article 58.7.(a) of the CSA, with a report to the CAB who issued the certificate;
 - the quality measures in place within the CAB, and the possibility to establish and handle complaints;
3. an assessment of the gravity of the irregularity by the CAB;

³ e.g., failure to describe some of the underlying capabilities that the service relies on.

⁴ e.g., advertising a certified cloud service after the product certificate has expired.

⁵ e.g., the introduction of new libraries or tools that may adversely impact security

⁶ e.g., a change in the tools in the development chain

⁷ At any time, the operated service must be the result of applying the processes described during the certification process to the service as it was certified.

4. using the possibility of the dialog between the CAB and the CSP to try and solve minor issues, and of the provisions of Chapter 13 (Non-Compliance) where necessary.

The NCCA shall be informed of the results of these activities.

In addition to the activities of market surveillance, the NCCA may establish rules for a periodic dialog between the issuers of certificates and the certificates owners, as to formally check and report the respect of previously stated obligations.

ENISA may provide for harmonisation into the EUCS scheme guidance on the commitments that may be part of an application request, with an indication of the associated gravity.

The following deviations shall be considered as potential issues related to non-compliance in the conditions under which the certification takes place and that are not related to the individual cloud service:

- failure to meet obligations regarding handling complaints towards maintaining the certificate validity, including:
 - obligations for auditing the scheme compliance of the CAB, its subcontractors and the certificate holders related to certificate use as implicitly required by Article 58.8.(b) of the EUCSA;
 - obligations for supervising and enforcing CAB's and certificate holder's scheme compliance as implicitly required by Art. 58.7.(a) of the EUCSA;
 - obligations for complaint handling as implicitly required by Art. 58.7.(f);
- deviations from evaluation requirements:
 - unjustified deviations from the evaluation methodology and applicable supporting documents described under Chapter 8 (Evaluation Methods and Criteria);
 - deviations from expected evaluation competence, as described under Chapter 7 (Specific requirements applicable to a CAB).

Such non-compliance in the conditions under which the certification takes place and that are not related to an individual cloud service shall:

1. be avoided where possible through:
 - the audits permitted through Article 58.8.(b) and (c) of the EUCSA;
 - the permanent monitoring of the CAB by their Accreditation bodies and of the CAB's subcontractors by the CAB and their Accreditation bodies, as requested by Chapters 7 (Specific requirements applicable to a CAB) and 22 (Peer Assessment);
2. be detected through:
 - the quality process of the CAB, including the report to the NCCA of the identified issue, and the requirement associated to their accreditation to handle complaints.

The following shall be considered as potential issues of non-conformity of a certified cloud service with its security requirements:

- a change in the cloud service itself leading to a change of the cloud service's security posture;
- a significant security incident that has affected the certified cloud service or has resulted in a data breach or loss of sensitive information;
- a change in the threat environment which has an adverse impact on the security of the certified cloud service;
- a vulnerability identified and related to the certified cloud service, that has an adverse impact on the security of the certified cloud service.

Such non-conformity of a certified cloud service with its security requirements shall be monitored under the following responsibilities:

1. CSPs shall:

- inform the CAB of major changes in the certified cloud service or in its Information Security Management System that may have an impact on the statements included in the related certificate;
 - monitor any vulnerability that would be relevant to their cloud service, either published by or received from end users and security researchers as defined in Article 55.1.(c), or discovered by the CSP, and submit an impact analysis where necessary to their CAB;
 - monitor the known dependencies and vulnerabilities identified by any other source that may apply to the certified cloud service, and submit an impact analysis where necessary to their CAB;
 - inform the CAB of any security incident that they notify to regulatory authorities;
 - work in cooperation with the CAB and where necessary with the NCCA to support their monitoring activities;
 - such activities may be assessed within the certification process of the cloud service, through the controls defined in the Incident Management category;
2. CABs shall;
- monitor any vulnerability from any source that would be relevant to their scope of evaluation and certification;
 - monitor the handling of incidents reported by CSPs; and
 - report to their NCCA any detected vulnerability affecting the conformity of a certified cloud service to the requirements related to the certification.

Where deemed necessary by the CAB or at the discretion of the NCCA, a series of evaluation tasks may be requested to be performed with the support⁸ of the CSP as to confirm the impact of a non-conformity.

These activities related to monitoring compliance shall be part of the annual summary report of a NCCA.

RATIONALE

Additional information from the EUCSA

Article 58, on NCCAs, includes:

7. National cybersecurity certification authorities shall:

- (a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

Article 59, on Peer reviews, includes:

3. Peer review shall assess:

- (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates pursuant to point (a) of Article 58(7);



The requirements have been established considering:

- potential irregularities (as of Article 56.8 of the EUCSA): An irregularity affecting a cloud service's conformity arises from the description of the service as stated in the certificate, or in the implementation of the controls described during the conformity assessment. Though such irregularities are addressed as a cloud service's non-compliance post-certification, they may arise any time;
- potential gaps into the technical competencies of a CAB;
- potential vulnerabilities and modifications of a cloud service or of its environment.

⁸ Where necessary, support shall imply financial support to described activities.

Associated non-compliance issues have been identified and counter-measures for the prevention and detection thereof established.

This process benefits of the provisions of the EUCSA:

- market surveillance installed by Article 58.7.(a);
- obligation on auditing the scheme compliance of CABs and certificate holders mandated by Article 58.8.(b);
- the right to contest certificates (Article 63.1), and the need to the responsible bodies or authorities to handle complaints regarding the validity of a certificate (Article 63.2), and therefore service compliance as required by Article 54.1.(j);
- the power of a NCCA – through the power of Article 58.8.(b) – to launch an audit of the certificate holder and issuer for any purpose related to their compliance to the European Cybersecurity Certification Framework.

As for the CSP's task to monitor the known dependencies and vulnerabilities: The Terms and Conditions of the certificate require that a CSP monitors the threat landscape and notifies the CAB about any vulnerability in their certified cloud service. A CAB or one of their accredited subcontractors may propose CSPs such a service.

As for the CSP's requirement to report to their CABs security incidents that they report to other regulatory authorities: the objective is to ensure that the CAB gets notified of significant incidents without adding a significant burden for CSPs during a crisis. So, no new criteria are here added.

Where necessary, the conditions to support new evaluation activities have been indicated, as they might have a financial impact.

Finally, the implementation of compliance monitoring by NCCAs may be the subject of peer review between NCCAs, as defined in Article 59; however, the peer review process is

12. CERTIFICATE MANAGEMENT

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

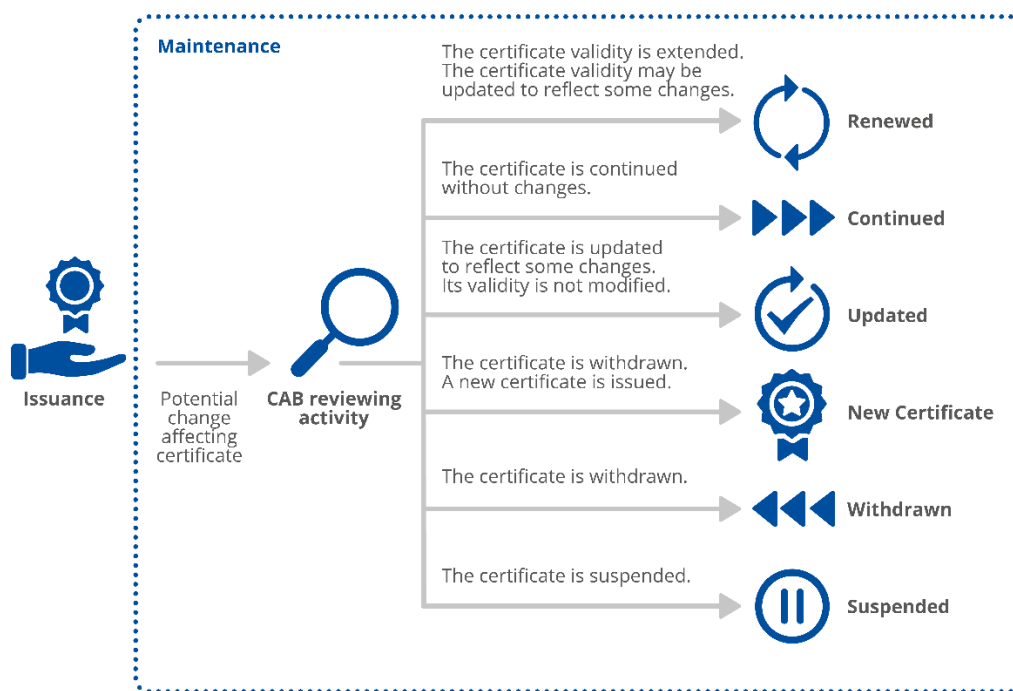
(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

Article 56 on Cybersecurity Certification also covers this issue:

9. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.



Figure 2: Processes related to the issuance and maintenance of a certificate



The reference standard for these activities is ISO/IEC 17065 and in particular, its Clause 7.10, where 'changes affecting a certificate' are discussed.

Conditions for issuing a certificate

A CAB shall only issue a certificate when:

- the applicant has committed to all obligations that need to be fulfilled under this scheme to obtain the certificate;
- the evaluation of the cloud service is successful and in line with the evaluation requirements set in this scheme in Annex B: (Meta-approach for the assessment of cloud services), Annex C: (Assessment for levels Substantial and High, and Annex D: (Assessment for level Basic) for the requested assurance level; and

- the review of the evaluation results is successful and in line with the requirements of ISO/IEC 17065 and with the requirements set in this scheme in Annex B: (Meta-approach for the assessment of cloud services) for the required assurance level.

The review shall be performed independently of the evaluation, and it shall cover all reports provided during the evaluation to ensure that the conclusions are consistent with the evidence adduced and that the accepted evaluation criteria and evaluation methods have been correctly applied.

The certificate shall be related to the version of the supplementary cybersecurity information produced by the vendor as specified in Article 55 of the CSA.

The CAB shall establish a period of validity for the certificate that shall not exceed the maximum period defined in Chapter 19 (Certificate validity).

Conditions for maintaining a certificate

During the validity period of the certificate, periodic reassessments are required to ensure that the CSP continues to fulfil the requirements set in this scheme. Such periodic reassessments shall not be separated by more than one year. This period may be reduced by the CAB if there are specific attention points that require an earlier reassessment.

Maintenance activities shall be initiated upon the following conditions:

- when the cloud service has been selected through the sampling rule installed for the general monitoring of certified cloud service, as defined by Chapter 11 (Compliance Monitoring) and Annex G: (Certification Lifecycle and continued assurance);
- following a confirmed nonconformity with security requirements, under the conditions defined in Chapter 13 (Non-Compliance);
- following an identified non-compliance with the accreditation requirements of the CAB, the CSA provisions, or the scheme requirements, that affects the certification.

Maintenance activities may be initiated on the request of the owner of the certificate upon one of the following conditions:

- a periodic reassessment is due to be performed;
- a renewal assessment is required to extend the validity period of the certificate;
- a change of the certified cloud service requires an update of the content of the certificate of the information published in compliance to Article 55(1);
- a significant change occurs in the certified cloud service or in the design and implementation of the security measures that fulfil the requirements of this scheme.

Depending on the nature of the previous conditions, and in accordance with the requirements established in Chapter 11 (Compliance Monitoring), Chapter 13 (Non-Compliance) and Chapter 14 (New Vulnerabilities), the maintenance activities shall be triggered at the discretion of the CSP, the CAB, or the NCCA. The National Accreditation Body may also trigger maintenance activities where a complaint has been issued.

When the maintenance activities are initiated by the CSP, the request to the CAB shall be accompanied with an Impact Analysis report (IAR), in accordance with Annex G:., Certification Lifecycle and continued assurance.

In all other cases when the maintenance activities are initiated by any other party (CAB, NCCA, and any stakeholder acting as a sponsor of the associated maintenance activities), the request shall be supported by a maintenance rationale containing a description of the potential or actual non-conformity or the identified non-compliance stated and its potential impact on the certificate.

Based on the IAR or the maintenance rationale and on the requirements defined in this scheme for re-assessment or renewal, the CAB shall validate whether some evaluation tasks are deemed necessary before its review and decision,

and validate accordingly the scope of and the workload associated to these tasks. The CAB shall also validate the result of the necessary evaluation tasks once completed.

Typical conformity assessment activities are defined in Annex G:, Certification Lifecycle and continued assurance:

- Periodic conformity assessment, including a partial re-assessment of the cloud service, to be performed at regular intervals, during the validity period of the certificate, as defined in Chapter 19, Certificate validity.
- Renewal conformity assessment, including a full re-assessment of the cloud service, to be performed before the expiration date of the certificate.
- Restoration conformity assessment, following a request from a CSP to consider changes in the certified cloud services, or following a request from a CAB or from the NCCA related to a nonconformity (Chapter 13, Non-Compliance) or to a new vulnerability (Chapter 14, New Vulnerabilities).

The CSP shall support⁹ the CAB for the conformity assessment activities deemed necessary, unless otherwise specified in Chapter 13 (Non-Compliance).

Upon review and decision of the CAB, the maintenance activities shall result in one the following decisions:

- continuing the certificate, corresponding to keeping the existing certificate alive, without change;
- updating the certificate to reflect some changes in the certified cloud service, including an extension of its scope;
- renewing the certificate with a new validity period and optionally some updates, corresponding to re-issuing the same certificate with a new validity period;
- withdrawing the certificate, and issuing a certificate with either a reduced assurance level, or a reduced scope of the certificate to still meet the current assurance level, potentially with a new validity period;
- suspending the certificate pending remedial action by the CSP;
- withdrawing the certificate.

Decisions shall be accompanied with a Maintenance Report issued by the CAB, in accordance with Annex G: (Certification Lifecycle and continued assurance), and uniquely linked to the certificate; it shall motivate the decision and, where applicable, indicate any necessary change to the initial certificate.

In the case no maintenance has been requested for a certificate that has reached its expiration date, in the case no maintenance has been requested when a periodic assessment is due, or more generally in the case a maintenance shall be initiated and no action was taken by any of the responsible parties in due time the certificate shall be suspended and the CSP notified of the non-compliance. If the CSP does not perform the maintenance in due time (as defined in Chapter 13, Non-Compliance), then the certificate shall be withdrawn.

All withdrawn certificates shall be subject to archiving. Archiving shall consist of still providing access to the certificate and associated information, with the clear indication of its withdrawal, for instance that its expiration date has passed.

The following table shall be considered by the CAB to support the appropriate decision on most frequent possible cases.

Table 4: Nominal decisions associated with the maintenance of certificates

Cases	Nominal decisions
The maintenance evaluation activities have been performed and reviewed, and have determined that the cloud service still fulfils the requirements without significant changes in the service	Continue the certificate until the next periodic assessment or until its expiration date

⁹ Where necessary, support shall imply financial support to described activities.

Cases	Nominal decisions
The maintenance evaluation activities have been performed and reviewed, and have determined that the cloud service still fulfils the requirements and the changes impact the security of users without any reduction in the scope of certification or assurance level	Update the certificate with the new information and continue the certificate until the next periodic assessment or until its expiration date
A renewal conformity assessment has been performed and reviewed, and have determined that the cloud service still fulfils the requirements, possibly with changes that impact the security of users without any reduction in the scope of certification or assurance level	Renew the certificate with a new expiration date and if required with the new information
The maintenance evaluation activities have been performed and reviewed, and have determined that the cloud service only fulfils the requirements after reducing the scope of certification or reducing the assurance level	Withdraw the certificate and issue a new certificate with the reduced scope or assurance level, possibly with a different expiration date
The maintenance evaluation activities have been performed and reviewed, have determined that the cloud service does not fulfil the requirements anymore, and action from the CSP is possible to maintain the certificate at the same assurance level and scope, though not immediately, or improper use of the certificate is not solved by suitable retractions and appropriate corrective actions by the CSP.	Suspend the certificate pending remedial action from the CSP
The maintenance evaluation activities have been performed and reviewed, and have determined that the cloud service does not fulfil the requirements anymore	Withdraw the certificate
The periodic assessment has not been performed in due time	Suspend the certificate pending remedial action from the CSP
Remediation action has not been performed in due time after suspension	Withdraw the certificate

A certificate shall only remain in the ‘suspended’ status for a maximum duration of 3 months that may only be extended with the explicit and motivated approval of the NCCA. In case no action is taken by the vendor in due time the status of certificate shall be changed into ‘withdrawn’ by the CAB.

Any change of the status of a certificate shall be disclosed without undue delay according to the requirements of Chapter 20 (Disclosure Policy).

RATIONALE

Requirements have been established considering the requirements associated with ISO/IEC 17065, and ISO/IEC 17067, Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes.

The full life cycle of a certificate, starting from its issuance with a defined validity period till its due or potential expiration (by validity period or preliminary to this due to a selection under the sampling rules for the general monitoring of certificates, a potential or actual non-conformity with security requirements, or an identified non-compliance with the accreditation requirements of the CAB, the EUCSA provisions, or the scheme requirements) has been considered.

One fundamental condition for issuing a certificate for the cloud service is successful evaluation, based on the present scheme. Other conditions stem from relevant provisions of the EUCSA, such as necessary authorizations for CAB based on Article 60.3 of the EUCSA which are external to the certification in its technical meaning, and may, if not fulfilled after certification, be considered as non-conformance cases.

All other certification activities are related to the phase after the certificate is issued, where ‘a *change affecting certification*’ occurs as mentioned in ISO/IEC 17065. These activities are described as ‘maintenance’. In that case, the CAB is obliged to act in response to a given trigger.

Wording from ISO/IEC 17065 describing all relevant activities related to the certificate which has been issued applies (see Clause 7.10).

13. NON-COMPLIANCE

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;



Chapter 11, Rules for monitoring compliance, defines several categories of non-compliance instances that may be uncovered through monitoring activities. When such non-compliance instances are uncovered, the consequences for the various stakeholders, including the CSP, the CAB and its subcontractors, and the NCCA, are as follows.

For confirmed deviations or irregularities associated to non-compliance by a CSP to the requirements related to a certificate issued on their cloud service, the following consequences shall occur in the general case:

- the CAB who has issued the certificate shall request the CSP for assertions and amendments to restore compliance, to be provided within the time frame of 14 days for certificates at the assurance level 'high', or 30 days for certificates at the assurance levels 'basic' or 'substantial';
- continued non-compliance past the allowed time frame shall trigger a suspension of the certificate for the cloud service, a suspension of all certification activities by the CAB on behalf of the CSP for other services, with information about the suspension by the CAB to the NCCA.

In the particular case of a confirmed deviation from the requirements of the certificate holder's obligations towards maintaining the certificate validity, or towards informing the appropriate authorities or bodies of any subsequently detected vulnerabilities, as requested by Article 56.8 of the CSA, the following consequences shall occur:

- an immediate suspension of the certificate, with information about the suspension by the CAB to the NCCA.

For a cloud service certified at assurance level High, in the case of a confirmed deviation from the requirements of the certificate holder's obligation of informing the appropriate authorities or bodies of any subsequently detected major nonconformity to the requirements of the scheme through continuous monitoring, the following consequences shall occur

- an immediate suspension of the certificate, with information about the suspension by the CAB to the NCCA.

The notification of the owner of a certificate of the suspension of the certificate shall mark the beginning of a suspension period of 14 days for certificates at the assurance level High, or 30 days for certificates at the assurance levels Basic or Substantial. During this period:

- the impact of the non-compliance on the certified cloud service shall be estimated with the necessary support¹⁰ of the CSP;

¹⁰ Where necessary, support shall imply financial support to described activities.

- when the non-compliance is verified to impact a certificate, this shall be treated as a non-conformity of the certified cloud service, the CAB who has issued the certificate shall request the CSP for assertions and amendments to restore compliance;
- the CSP shall accept or refuse the handling of the verified nonconformity and the associated maintenance activities, as defined in Chapter 12 (Conditions for issuing, maintaining, continuing and renewing certificates);
- when the handling is refused, the certificate shall be withdrawn;
- when the handling is accepted, the CSP shall proceed to the necessary changes to the cloud service
- when the defined period is not sufficient for the above described task, the issuer of the certificate, upon receiving a duly justified request, may extend the grace period, no more than three times the above described duration;
- when necessary (e.g. lack of availability of the CAB), the CAB may decide to further extend the suspension period up to a maximum of 90 days;
- if at the end of the suspension period, the handling of the verified non-conformity and the associate maintenance activities have not been completed, then the certificate shall be withdrawn.

ENISA shall be informed for publication on its website, and provided with all the information to be published:

- at the suspension of the certificate;
- at any extension of the suspension period;
- at the end of the suspension of the certificate;
- at the withdrawal of the certificate.

In the case of a suspension or of the extension of a suspension, the information provided to be published to ENISA shall include at least the end date of the suspension period, the reason for the suspension, and recommendations for the users of the certificates.

The NCCA shall be informed at any extension of a suspension period.

For a confirmed non-compliance in the conditions under which the certification takes place and that are not related to the individual cloud service, the concerned CAB shall proceed, under the control of the NCCA, to the following:

- the identification, with the support of relevant teams and subcontractors, of potentially impacted certified cloud services;
- where deemed necessary by the CAB, or at the discretion of the NCCA, the request for a series of conformity assessment activities to be performed on one or more cloud services by either the CAB or subcontractor who performed the audit or any other CAN or subcontractor that would be in a better technical position to perform these activities, leading to updated assurance reports;
- the review by the CAB of the updated assurance reports, and where necessary, the re-issuance of certificates in accordance with the requirements of Chapter 12 (Conditions for issuing, maintaining, continuing and renewing certificates), or the notification to the CSPs of the impacts of the non-compliance on their certificates.

These activities shall occur within the maximum period of 14 days for certificates at assurance level High or 30 days for certificates at assurance levels Basic and Substantial, which may only be extended after approval by the NCCA.

When a CAB or the NCCA mandates new evaluation activities to be performed, these activities and the related review and issuance activities shall be supported¹¹ by the CAB that proved to be non-compliant¹².

Where impacts are confirmed to affect a certificate, they shall be treated as a nonconformity of the certified cloud service, following the above-defined rules.

¹¹ Where necessary, support shall imply financial support to described activities.

¹² Or by a subcontractor of the CAB if that subcontractor proved to be non-compliant in breach of its contractual obligations.

RATIONALE

Additional information from the EUCSA

Recitals provide additional information:

(65) National cybersecurity certification authorities should in particular monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes established in its respective territory in relation to the EU statement of conformity, should assist the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies by providing them with expertise and relevant information, should authorise conformity assessment bodies to carry out their tasks where such bodies meet additional requirements set out in a European cybersecurity certification scheme, and should monitor relevant developments in the field of cybersecurity certification. National cybersecurity certification authorities should also handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by those authorities or in relation to European cybersecurity certificates issued by conformity assessment bodies, where such certificates indicate assurance level 'high', should investigate, to the extent appropriate, the subject matter of the complaint and should inform the complainant of the progress and the outcome of the investigation within a reasonable period. Moreover, national cybersecurity certification authorities should cooperate with other national cybersecurity certification authorities or other public authorities, including by the sharing of information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with specific European cybersecurity certification schemes. The Commission should facilitate that sharing of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the Rapid Alert System for dangerous non-food products (RAPEX), already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.



This is a rather simple set of rules:

- The main ruleset is about non-conformity in the cloud service (and its operation). The way in which it is discovered is not mentioned here, most likely through monitoring or complaints.
 - In that ruleset, the CSP has an opportunity to fix the issue without any visible consequence (no suspension, no withdrawal).
 - If they fail to do this timely, then a suspension occurs.
 - There is one exception, when a CSP fails in its continued assurance and maintenance duties; then, the suspension occurs directly. This is intended to highlight the responsibility of the CSP to continue working on security after the issuance of the certificate; also, it highlights the fact that, at that stage, the CAB only gets involved (with an opportunity to perform evaluation activities) if the CSP reports issues as planned.
- The second ruleset is about what happens when a suspension occurs (directly or after failure to act swiftly when a non-conformity is discovered).
 - Another delay starts running, this time with notification of the NCCA, and with publicity through ENISA's Web site (including automated notification of customers who have registered for updates on the certificate with ENISA).
 - If need be, the delay can be extended, when duly justified. The NCCA is notified of extensions, and my signal at some point that "enough is enough".
 - When the delay expires, withdrawal occurs; withdrawal may also occur if the CSP refuses to implement corrective actions.
- The third ruleset is about what happens when a CAB fails to do their work properly.
 - All certificates issued by that CAB have to be reviewed. That review may involve some work.
 - If that review shows that certificates are impacted, then some evaluation work may need to be redone, as well as the corresponding review work, and if needed, the modification of the certificate.

- CSPs are notified when their certificates are impacted, but they are not held directly responsible for the work that needs to be redone. However, if a non-conformity is identified in their cloud service during that review, then this non-conformity needs to be handled following the first ruleset (and the second if needed).

In all cases, the entity responsible for the non-conformity is responsible for supporting the additional work, including, but not limited to, additional costs.

14. NEW VULNERABILITIES

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;



Vulnerability handling

CSPs shall use the general steps of ISO/IEC 30111 for vulnerability handling: preparation, receipt, verification, remediation development, release, post release, with the following specific application rules for the EUCS scheme. These rules are defined in the present chapter, as well as in the definition of the security controls related to incident management, in Annex A: (Security Objectives and requirements for Cloud Services).

PREPARATION

CSPs shall develop methods for receiving vulnerability information and make them public in accordance with Article 55.1.c) of the CSA.

RECEIPT

In the following cases where:

- the CSP of the certified cloud service receives vulnerability information according to Article 55.1.(c) of the EUCSA;
- there is a new publicly disclosed vulnerability on the referenced online repositories according to Article 55.1.(d) of the EUCSA;
- the CSP finds out a related vulnerability to its certified cloud service in any other way,

The CSP shall start handling the vulnerability according to its defined policies and procedures. If the vulnerability analysis determines that the risk for the cloud service related to the vulnerability is major¹³, then the CSP shall report without delay to the CAB that issued the certificate a description of the vulnerability, together with a description of its impact.

The time between the CSP learns about the vulnerability and the notification of the CAB shall not exceed five (5) working days. Failure to notify the CAB of a vulnerability with major impact or to do so within five (5) working days shall be considered as a non-compliance to the rules of the scheme, as defined in Chapter 13 (Non-Compliance).

At the time the CSP notifies the CAB, the analysis of the vulnerability may not be finalized. In such a case, the CSP shall provide to the CAB a delay for the delivery of the full analysis, which shall not exceed ninety (90) days after the CSP became aware of the vulnerability.

The information may contain details about the possible exploit(s) of the vulnerability: in that case, it shall carry the appropriate TLP classification as to ensure the relevant protection, in accordance with the standard rules defined in

¹³ According to the CSP's own vulnerability assessment scale, which shall be defined as part of its vulnerability handling policy, as required in Annex A: Security Objectives and requirements for Cloud Services, and shall consider the potential impact and the likelihood of exploitation of the vulnerability in the context of the cloud service.

<https://www.first.org/ttp/>, or with alternative classification and mechanisms previously agreed between the CSP and the CAB.

VERIFICATION AND REMEDIATION DEVELOPMENT

In addition to the security controls defined in Annex A: (Security Objectives and requirements for Cloud Services), the CSP's processes shall include the following steps:

- In its analysis of the vulnerability with major impact, the CSP shall propose (1) whether or not the certificate should be suspended until a remediation is released, and (2) whether or not a restoration conformity assessment should be performed on the cloud service after remediation. The CAB shall agree on the proposed actions or make alternative proposals within five (5) working days. When both parties deem necessary or are unable to agree on such decisions, they may inform the NCCA and ask for its advice.
- If a maintenance conformity assessment has been deemed necessary, it shall be performed before lifting a potential suspension of the certificate.

RELEASE AND POST-RELEASE

There are no specific rules related to these phases, beyond the requirements defined in Annex A: (Security Objectives and requirements for Cloud Services).

Vulnerability disclosure

CSPs may use the following standard as for the general rules related to vulnerability disclosure:

- ISO/IEC 29147 Information technology – Security techniques – Vulnerability disclosure.

During the vulnerability analysis, the cloud service may apply an embargo period, meaning that the possible vulnerability is not further disclosed. This period shall not last longer than three (3) months. The NCCA may, however, consider extending this period when a justified request is received, in particular when it is confirmed that time must be given to downstream vendors integrating the cloud service for analysing the impact of the vulnerability (both from a technical and certification point of view).

In addition to the general disclosure rules above, once a strategy to correct the issue has been defined by the CSP with the approval of the CAB, information related to the confirmed vulnerability shall be disclosed to the NCCA, in accordance with Article 56.8) of the CSA.

The information shall not contain details about the possible exploit of the vulnerability. It shall contain the necessary elements for the NCCA to understand the impact of the vulnerability, the changes to be brought to the cloud service, and where applicable, information by the CAB on the broader applicability of the vulnerability to other certified cloud services.

The NCCA shall in accordance with Article 58 7 h) share this information with the other NCCAs, which may also decide to further analyse the problem or, after informing the CSP about the information exchange, ask the related CABs to analyse whether further certified cloud services are affected. This information exchange shall be done in confidentiality, including application of encryption and need-to-know principle.

When a correction has been brought to the certified cloud service, the CSP shall establish the necessary CVE with the support of the NCCA and related national CSIRT, and proceed to its publication on the relevant list, in accordance with the requirements of Article 55 of the CSA. ENISA shall be informed of the changes of status of the related certificates.

NCCAs may develop their capacity to act as “coordinators” as defined in ISO/IEC 29147, and alternatively, designate their national CSIRT to play this role. In that case, the CSIRT shall have access to the necessary details related to the vulnerabilities and to the certificated cloud services.

RATIONALE

The current description has been strongly inspired from the EUCC, with a few significant simplifications. In particular, there is no mention of an attack potential in the analysis of a vulnerability.

This requirement has been replaced by a decision about the suspension and the need to perform another conformity assessment (which is only expected when an incident is linked to a dysfunction in the application of processes).

15. RECORD RETENTION

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (n) where applicable, rules concerning the retention of records by conformity assessment bodies;



Each CAB shall maintain a records system in accordance with the requirements of the accreditation standard ISO/IEC 17065 (or to the applicable accreditation standard for its internal or external evaluation facilities, e.g. ISO/IEC17021-3).

The records system shall include all records and other documents produced in connection with each conformity assessment, as well as documents and evidence provided by the CSP about the implementation of security controls; the record system shall also include a list of all the documents and evidence made available temporarily by the CSP during the conformity assessment. It shall be sufficiently complete to enable the course of each certification to be traced.

All records shall be securely and accessibly stored for a period of at least seven (7) years after the expiration or withdrawal of the certificate.

In case a later expiration date of the certificate is attributed in accordance with the conditions of Chapter 12 (Certificate Management), it shall be taken into account for the new calculation of the retention period of the records, with the same rule as previously stated. New or revised information related to the activities described under Chapter 12 (Certificate Management) shall be added to the previous records for the certificate.

RATIONALE

The proposal consists in to require records to be kept for seven (7) years after the expiration of the certificate, or until legal actions related to the certificate are completed.

If the certificate is renewed, then the records are kept for seven (7) years after the new date, with a full history of the certificate, including records related to all conformity assessments.

Also, there is a split responsibility between the CAB and the CSP regarding the documents and evidence that the CSP made available in a restricted manner to the CAB: It is the CSP's responsibility to keep these records, while the CAB only maintains a list of the documents.

16. RELATED SCHEMES

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;



Within the EU, the following national cybersecurity certification schemes cover the same type or categories of services:

- The SecNumCloud scheme in France, operated by ANSSI:
<https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/>
- The C5 methodology in Germany, defined by BSI:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog_node.html
- The Zeker-Online scheme in the Netherlands, operated by the Zeker-Online foundation:
<https://www.zeker-online.nl>

These schemes only provide a partial coverage of the requirements provided in the present scheme, and they also include some requirements that have not been included in the present scheme¹⁴. In particular, each scheme defines only a single assurance level.

Nevertheless, it shall be considered that:

- a certificate issued under these schemes may where necessary¹⁵ be transformed into a certificate under the EUCS scheme if all required activities are conducted;
- a CAB may accept to use the results of evaluation activities performed under these schemes for a certification under the EUCS scheme;
- a certificate issued under these schemes may be used for certifications under the EUCS scheme whereby the CSP uses the certificate as assurance documentation for subservice organizations until its period of validity, if evaluation work confirms that the subservice meets all requirements of the EUCS scheme.

ENISA may establish associated guidance as to support the conditions related to these possibilities. This guidance shall be established in cooperation with the ECCG.

Based on the recommendations established by this Chapter, the European Commission and EU Member States may consider to establish a date of one (1) year after the implementing act has been adopted pursuant to Article 49(7) for existing schemes to cease producing effect.

¹⁴ In most cases, the requirements that have not been included are related to aspects beyond security, to aspects that are not relevant in a cybersecurity certification scheme, for instance related to procurement, or to aspects that are covered differently in the EUCS scheme.

¹⁵ To satisfy market or regulatory requirements.

Some of these schemes may continue to run conformity assessment activities covering the same type or category of ICT services, security requirements, evaluation criteria and methods and go beyond the scope of the EUCS scheme in terms of assurance levels or requirements.

Further to these National schemes, no international schemes have been identified that cover the same services, security requirements, evaluation criteria and methods.

RATIONALE

Additional information from the EUCSA

Article 57 provides additional information regarding National cybersecurity schemes and certificates:

1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.
2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services and ICT processes already covered by a European cybersecurity certification scheme that is in force.



We acknowledge in this chapter that there were pre-existing schemes in Europe; these schemes were very different in nature, in some cases not even issuing any kind of declaration (like Germany's C5). Nevertheless, the companies who went through a conformity assessment using one of these schemes have been gathering evidence, which led to an analysis by a CAB, and some of this information may be relevant for EUCS conformity assessments.

Out of the three reuse hypotheses included, the first one (transformation of a certificate) is the least likely to be used, because the differences are quite significant. The reuse of evidence and of evaluation results, though, could lead to significant optimizations of the evaluation process. Finally, the use of previously issued documentation (certificates, reports) as a basis for composition may allow smaller vendors, who rely on someone else's infrastructure to get started earlier with their certification.

Regarding the details of such reuse, we are following the path set by the EUCC scheme by allowing these details to be provided later, in a guidance issued by ENISA and elaborated with the Member States through the ECCG.

We have also proposed to delay the issuance of certificates through the scheme for one year, giving the community enough time to develop the required guidance. This is covered in greater details in Chapter 25 (Further Recommendations).



17. CERTIFICATE FORMAT

Foreword for Reviewers

This chapter is still work in progress.

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;



RATIONALE

A proposal for the Certification Report format is included in Annex F: (Scheme Document Content requirements). A proposed format for the certificate itself will be added later.

18. AVAILABILITY OF INFORMATION

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;



Each CSP shall maintain a publication system for the information to be made available to the public, in accordance with the procedures described in Chapter 23 (Supplementary Information) for the Supplementary cybersecurity information.

All information shall be available for a period of at least seven (7) years after the expiration or withdrawal of the certificate.

In case a later expiration date of the certificate is attributed in accordance with the activities described under Chapter 12 (Certificate Management), it shall be taken into account for the calculation of the availability period of the information, with the same rule as previously stated.

Available information shall be updated with the new or revised information related to the activities performed under Chapter 12 (Certificate Management).

Records of information made available to the CAB for the conformity assessment process shall be stored securely, and made available on its request to the CAB or the NCCA (according to Article 58.8(a) of the EUCSA) up to five years after expiration of the certification, in line with the duration established under Chapter 15 (Record Retention). These records shall include all documentation and evidence made available to the CAB during the conformity assessment, including those that were only made available in a restricted manner, for a limited time or only on the CSP's premises.

Over the period of validity of a certificate, some of the information associated to the cloud service may be deprecated and replaced by new information, and the need to maintain available information on the cloud service only relates to the valid and up-to-date information. The deprecated information shall still be archived for the duration of the related certificate when the information was deprecated plus seven (7) years.

RATIONALE

The period of retention for CSPs shall not be shorter than the retention of records by the CAB that is of seven (7) years after the end of validity period of the certificate. This applies in particular to the information made available in a restricted manner to the CAB, which is retained under the sole responsibility of the CSP, whereas the CAB only maintains a list of the records made available).

It is to be noted that CSPs may however have to extend this period, in order to comply with other regulations that state a different period of availability of documentation, up to ten (10) years.

19. CERTIFICATE VALIDITY

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (r) maximum period of validity of European cybersecurity certificates issued under the scheme;



The maximum period of validity of the certificates shall be three (3) years. In order to maintain the validity of the certificate for its full period of validity, the CSP shall follow the processes defined in Chapter 12 (Certificate Management), and the certified cloud service shall be subject to a periodic conformity assessment or to a renewal conformity assessment at most one (1) year after the previous initial, periodic, or renewal conformity assessment.

Under certain conditions, and following the processes defined in Chapter 12 (Certificate Management), a CAB may continue a certificate with an extended validity period beyond the initial three (3) years.

RATIONALE

According to the large variety of cloud services that can be certified under this scheme, to their and evolution (often with frequent updates), to the various levels of assurance that can be achieved and the associated effort to generate assurance that the scheme's requirements are fulfilled, an average maximum of three (3) years was selected for the general case.

Since this is a maximum, it remains possible to issue a certificate for a shorter period of time, in particular if the CAB believes that issuing a certificate for three (3) years would lead to potential risks.

The chapter also defines the 1-year limit between periodic assessments. This limit applies to all levels, but the nature of the activities to be performed depends on the level.

20. DISCLOSURE POLICY

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;



The certificates shall be disclosed by ENISA, with the related certification report and any relevant information as requested by other chapters of this document, in a dedicated website on European cybersecurity certification schemes, in accordance with Article 50.1 of the CSA.

The certificates shall be disclosed with their applicable status, as decided through the application of the requirements established by Chapter 12 (Certificate Management) and Chapter 13 (Non-Compliance).

The certificates may also be disclosed by the NCCAs and the issuing CABs on their websites. Any change to the status of a certificate shall be reported to the NCCA and to ENISA.

Amendments and withdrawals of certificates resulting from maintenance activities shall as well be published, in a way that users of certificates can identify which versions of a certified cloud service are certified (where applicable) and which relevant information shall apply (such as guidance).

ENISA shall establish in cooperation with the ECCG the conditions and/or guidance for the delivery and for the publication in due time of certificates and their updates, and associated relevant information, and shall make them publicly available on its website dedicated to cybersecurity certification.

Such information on the website on European cybersecurity certification schemes shall be available in English language. It shall be available at least for the entire period of validity of the certificate.

The certificates may be complemented with additional information, such as a QR-code providing a direct link to the corresponding certificate and related information, as to offer a better user experience and to publicise the certificates. ENISA may therefore establish a procedure for the generation of a QR-code: such procedure may imply that CABs, ahead of the release of a certificate, request from ENISA the generation of the QR-code to be applied on the certificate and provided to the CSPs for their commercial and technical documents.

CSPs may use certificates published on ENISA's website for commercial purposes, but they shall not modify the certificate, and in particular, they shall always include a link to the original certificate on ENISA's website to allow customers to check the current status of the certificate. Only cloud services with a valid certificate shall be promoted as certified cloud services by their relevant CSP, or users of these services.

If a certificate is suspended, the information published on ENISA's website shall include the date of the end of the suspension period, a reason for the suspension, as well as recommendations for the users of the certificate.

Once a certificate has expired or has been withdrawn, ENISA shall move it to a dedicated archive part of the website, where it shall remain available for at least (5) years. CSPs shall not refer to such expired or withdrawn certificates in their commercial information, and any access to the expired or withdrawn certificate through its initial URL or QR-code shall lead to the prominent display of the current status of the certificate.

RATIONALE

ENISA will publish the certificates with appropriate relevant information attached. To manage accurate and up to date dataflows, ENISA will establish conditions and/or guidance for the delivery and publication of information.

In accordance with Chapter 17 (Certificate Format), both certificates and associated certification reports, as well as relevant information for the secure configuration and usage of the certified cloud service (guidance) shall be made available to the users (and potential users) of certificates. Amendments to certificate will also need to contain the same type of information as the issuance of certificates, including guidance, and users shall be given an easy access to the status of the certificates when using ENISA dedicated Website.

As to offer an easy access to the Supplementary cybersecurity information defined by Article 55, a validated link to that information will be made available into the certificate.

ENISA shall be informed without undue delay of the evolution of the certificates, be it an amendment or a withdrawal, in line with the requirements of relevant Chapters of this scheme and Recital 93 of the CSA.

As to offer the necessary flexibility and enforcing character of the conditions for presentation of the information to ENISA, and for its publication, ENISA will establish generic conditions and/or guidance.

The generic conditions and/or guidance should make sure information is accurate and up to date as the information provided by ENISA could act as a single point of reference. It should define what information is to be transmitted to ENISA and within what reasonable timeframe. According to principles of transparency and openness, the outlines of these conditions/guidance should be made public on the ENISA Website.

As to promote valid certificates, certificates that have expired will be archived and made available on a different webpage than the valid ones.

21. MUTUAL RECOGNITION

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

- (t) conditions for the mutual recognition of certification schemes with third countries;



The mutual recognition of certification schemes with third countries shall be supported by the establishment of a Mutual Recognition Agreement (MRA) between the participants.

This MRA may include the following information:

- participants to the MRA;
- purpose and spirit of the Agreement;
- membership;
- scope;
- exceptions;
- definitions;
- conditions for recognition of certificates;
- peer assessments;
- publications;
- sharing of Information;
- acceptance of new participants and compliant authorities or bodies;
- administration of this Agreement;
- disagreements;
- costs of this Agreement;
- revision;
- duration;
- voluntary termination of participation;
- commencement and continuation;
- effect of this Agreement.

Conditions for recognition of certificates by participants to such an Agreement shall include at a minimum the following conditions:

- the participants shall commit themselves to recognise applicable conformant certificates by any accepted Participant;
- acceptance of participants shall confirm that the evaluation and certification processes have been carried out in a duly professional manner:
 - on the basis of commonly accepted ICT security evaluation criteria;
 - using commonly accepted ICT security evaluation methods;
 - in the context of an evaluation and certification scheme managed by a compliant certification body in the accepted participant's country;
 - the conformant certificates and certification reports issued satisfy the objectives of this Agreement;
- certificates which meet all these conditions shall be termed as conformant certificates for the purposes of this Agreement;

- ICT security evaluation criteria are to be those laid down in Chapter 8 (Evaluation Methods and Criteria) of this document;
- minimum requirements for Certification Reports are laid down in Annex 13 to this document;
- the scheme of the participants or to which the participants adhere shall be organised with a proper National Authority and conformity assessment bodies (CABs), in accordance with the following requirements:
 - the National Authority supervises the certification activities, notifies and authorises where applicable CABs, and reports any vulnerability of certified cloud services to the NCCAs of the EU participants;
 - the CAB has been accredited in its respective country by a recognised Accreditation Body in accordance with ISO/IEC 17065 and has been authorised where necessary by the National Authority;
 - the CAB is accepted as compliant by the Participants through a peer assessment mechanism installed for the MRA;
 - the CAB has been where necessary subject to an assessment by the National Authority in order to confirm its competence to perform evaluations, in accordance with Chapter 7 (Specific requirements applicable to a CAB) of this document;
- in order to assist the consistent application of the criteria and methods between evaluation and certification schemes, the participants plan to work towards a uniform interpretation of the currently applicable criteria and methods and commit to accept the supporting documents that results from this work. In pursuit of this goal, the participants also plan to conduct regular exchanges of information on interpretations and discussions necessary to resolve differences of interpretation;
- in further aid to the goal of consistent, credible and competent application of the criteria and methods, the certification bodies shall undertake the responsibility for the monitoring of all evaluations in progress within the MRA at an appropriate level, and carrying out other procedures to ensure that all CABs:
 - perform evaluations impartially;
 - apply the criteria and methods correctly and consistently;
 - have and maintain the required technical competencies;
 - adequately protect the confidentiality of sensitive or protected information.

The MRA may include a limitation of the assurance level of the certificates subject to recognition.

CAB(s) of the participants of such an Agreement that issue(s) certificates at the equivalent assurance level 'high' of the CSA shall be subject to peer assessments in line with the procedure set up in this scheme (Annex H; Peer assessment).

The procedure may be adapted and simplified for the CABs that issue certificates at the equivalent assurance levels 'basic' or 'substantial' of the CSA as to benefit from the international Accreditation system, and shall at least consist of the following activities by the peer assessment team regarding review of the:

- documentation associated to 2 certification projects of the 'substantial' assurance level;
- procedures associated to the security of information.

RATIONALE

Additional input from the EUCSA

The context for mutual recognition is provided in the EUCA recitals:

(104) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries.

The text is here strongly inspired from the EUCC scheme, around which some MRAs already exist. In the context of the EUCS scheme, a number of parameters, including the evaluation criteria and methods, are specific to the scheme; mutual recognition is therefore likely to be possible only with third countries that will operate a scheme locally that use the criteria and methods defined in the EUCS scheme.

22. PEER ASSESSMENT

ARTICLE 54 REFERENCE

Article 54. A European cybersecurity certification scheme shall include at least the following elements:

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;



The EUCS scheme requires that each authority¹⁶ or body issuing certificates at the assurance level High undergo a peer assessment at periodic intervals.

While every authority or body issuing certificates for assurance level 'high' pursuant to Article 56.6 of the EUCSA, including their subcontractors, shall operate under its own responsibility, a peer assessment shall be established for those issuing EUCS certificates at level High to:

- assess that they work in a harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composite service certification, as offered by Chapter 3 (Purpose of the scheme), including the reuse of a certified cloud service's evaluation results when used as base component in a composite service;
- identify any potential strength that result out of their daily work and that may benefit to others;
- identify any potential weakness that result out of their daily work and that shall to be considered for improvement by the peer assessed CAB;
- find a harmonised way to handle nonconformities and vulnerabilities and exchange best practices regarding the handling of complaints.

Note: The peer assessment is not intended to interfere with or make judgement to the activities performed by the NCCA, as this is the subject of the peer review process as required by Article 59 of EUCSA. Nor shall it interfere with or make judgement to the activities performed by the National Accreditation Body (NAB).

In order to allow timely feedback with respect to questions of the national aspects of the scheme that are handled by the NCCA, a representative of the NCCA of the assessed CAB shall participate to the peer assessment.

The peer assessment of each CAB issuing certificates of assurance level 'high' shall take place on a regular basis, with a periodic interval that shall not exceed five (5) years.

The ECCG¹⁷ shall establish and maintain a planning of peer assessments ensuring that this periodicity is respected, and take into consideration the level of priority that may be given to the peer assessment of a CAB issuing certificates at the assurance level 'high' in case of alleged non-compliance of this CAB, and in case of CBs with recent activity engaged in certifications for the first time or after a long lasting break (more than two years).

¹⁶ From the perspective of peer assessment, an authority that is issuing certificates as the assurance level high should be considered as a CAB, and participate in the same way to peer assessment.

¹⁷ The ECCG may establish a dedicated subgroup to handle peer assessments, based on the organisation to be installed for the maintenance of the EUCS scheme (see Chapter 25, Further Recommendations).

In the case of Article 56.6.(a) of the EUCSA, both the CAB issuing the certificates and the NCCA proceeding to the prior approval for each individual certificate shall be subject to the peer assessment. This shall include the procedure established by of the NCCA for prior approval for each individual certificate.

In the case of Article 56.6.(b) of the CSA, both the CAB issuing the certificates and the NCCA shall be subject to the peer assessment. This shall include the general delegation requirements defined by the NCCA.

Peer assessments shall follow the procedure established in Annex H: (Peer assessment). Unless duly justified, peer assessments shall be performed on site for the peer assessed CAB and, where applicable, for a selected set of its subcontractors.

The peer assessment team may decide to reuse results of previous peer assessments of the assessed authority or body covering part of the scope, under the following conditions:

- such results shall be not older than five (5) years;
- where previous peer assessments of the peer assessed CAB were performed under a different scheme, these shall be provided with the description of the peer assessment procedures in place for that different scheme;
- the peer assessment report shall clearly indicate which parts were reused without further assessment, and which parts were reused with additional assessment;

The peer assessment team shall report their findings to the ECCG in a peer assessment report, with an indication of the severity of any shortcomings. The peer assessment report shall include where necessary guidelines or recommendations on actions or measures to be taken by the peer assessed CAB, as well as the measures proposed by the peer assessed CAB to handle the findings.

When establishing measures to handle the findings, the peer assessed CAB may ask for the support of the peer assessment team. These measures shall be transmitted to the ECCG, indicating how they intend to correct the findings, within the peer assessment report. Where necessary, the ECCG may inform the relevant:

- NCCA of the peer assessed CAB for its consideration of the potential impact of the remaining findings on the certificates issued by the peer assessed CAB, or any authorisation or notification related to the peer assessed CAB and associated subcontractors;
- National Accreditation Body (NAB) of the peer assessed CAB for its consideration of the potential impact of the remaining findings on the accreditation of the peer assessed CAB and associated subcontractors;

and may ask for their conclusions.

The peer assessed CAB and related NCCA shall have the opportunity to address with the ECCG any shortcomings and recommendations identified in the report, before the results of the peer assessment are published by ENISA. Also, the NAB shall have the opportunity to address any shortcomings and recommendations in case any have been brought up to the NAB before the results are published.

ENISA may participate in the peer assessments.

CABs shall inform applicants to certification at the assurance level High of the EUCS scheme that their certification projects may be subject to the peer assessment installed by this scheme.

RATIONALE

Additional input from the EUCSA

Additional information about peer assessment is provided in the EUCA recitals:

(100) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the European cybersecurity certification framework, certain European cybersecurity certification schemes may include a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services and ICT processes with an assurance level 'high' under such schemes. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way, and may include appeal mechanisms. The results of the peer assessments should be made publicly available. The bodies concerned may adopt appropriate measures to adapt their practices and expertise accordingly.



In addition to the peer review between NCCAs, introduced in Article 59 of the EUCSA, which is outside of the scope of this scheme, a peer assessment may be defined for each scheme, with scheme specific objectives defined here for the EUCC scheme in the first part of this Chapter, and requirements.

This approach guarantees the high quality of evaluation activities as required for a 'high' level of security assurance and the harmonisation of the evaluation methods between different CAB, therefore allowing more objective results and to proceed to composite cloud service certifications within different CABs.

It is essential that a planning is established for such activities, including reassessments, and necessary priorities associated to newcomers to certification, or those facing issues with certification.

The procedure in Annex H: (Peer assessment) takes into consideration the possibility to reuse results from other peer assessment mechanisms.

The results of the peer assessment will be made publicly available on the ENISA website dedicated to cybersecurity certification, as recommended by Recital 100 of the CSA.

It is considered of importance that where applicable, the assessed body or authority presents the effective measures to adapt their practices and expertise accordingly to the ECCG, in order to reinsure other participants to the scheme of the quality of the certificate it issues.

In cases where the quality of the certificates is considered by the ECCG not in line with the requirements of this scheme, the ECCG may inform and consult the NCCA and the National Accreditation Body of the assessed body or authority for their conclusions on the impacts on its authorisation and accreditation.

23. SUPPLEMENTARY INFORMATION

ARTICLE 54 REFERENCE

A European cybersecurity certification scheme shall include at least the following elements

- (v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.



All Supplementary cybersecurity information defined in Article 55 of the EUCSA shall be provided during conformity assessment by CSPs to the CAB in the course of the conformity assessment.

In particular, in accordance with the requirements of Chapter 17 (Certificate Format), a link to the website and relevant pages where that information is made available shall be provided to be integrated into the certificate. Once all other requirements for certification have been fulfilled, the issuing body shall request the CSP to provide the URL (link) so that this can be processed before the certificate can be uploaded to the ENISA Website for certification.

CSPs shall make Supplementary cybersecurity information in accordance with Article 55 of the EUCSA publicly available on their websites.

The information shall be available in electronic form and in English language and shall remain available at least until the expiration or withdrawal of the corresponding European cybersecurity certificate. It shall be updated in accordance with the requirements of Chapter 12 (Certificate Management).

In addition, “guidance and recommendations¹⁸ to assist end users with the secure configuration, installation, deployment, operation and maintenance of the cloud services”, as defined by Article 55.1.(a), shall be updated as required to reflect the evolution of the cloud service, in accordance with the requirements of Chapter 12 (Certificate Management).

¹⁸ Within the shared responsibility model, these recommendations only cover the part for which the CSC is responsible. Recommendations for activities under the responsibility of the CSP do not need to be made publicly available.

RATIONALE

Additional input from the EUCSA

Article 55 defines the Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes:

1. The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:
 - (a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;
 - (b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;
 - (c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;
 - (d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.
2. The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.



In addition to the public availability of the information, as requested by Article 55, the need for having access to all or part of it during certification may be requested, such as to test that the information complies with the requirements of the scheme. The CSP should have the URL up and running before the certificate is issued or updated, and provisioned with the information provided for the conformity assessment. This specific need to review part of Supplementary cybersecurity information during the conformity assessment phase shall however only occur where the relevant Chapters of this scheme establish a requirement to do so.

For an easy and harmonised access of users of certificates to the webpages where the information will be accessible on the Websites of CSPs, the associated link will have to be provided in the certificate.

The conditions to deliver the Supplementary cybersecurity information should be part of a more detailed disclosure policy that ENISA will establish in accordance with the requirements of Chapter 20 (Disclosure Policy).

24. ADDITIONAL TOPICS

Foreword for Reviewers

This chapter introduces a few topics that are not addressed in Article 54, but may still be relevant for the present scheme. The topics do not all have the same level of maturity:

The two first ones (Security Profiles and Force Majeure) are high-level proposals that need to be further detailed and instantiated in the scheme, whereas the two last ones (Security of Information and Composition) are more mature, and are ready to be integrated in the scheme.

24.1 SECURITY PROFILES

PROPOSAL

Cloud services are likely to be used in ICT products, ICT services and ICT processes that will themselves be subject to certification in the context of another conformity assessment scheme, and in particular of another European cybersecurity certification scheme. Some of these conformity assessment schemes may have specific requirements, for instance related to an industry vertical.

In order to simplify the use of certificates issued in the EUCS scheme in other schemes, it is therefore important to support the definition of such specific vertical requirements, and to allow cloud services to take these requirements into consideration in their certification.

Such specific requirements shall be defined in a Security Profile, following some principles:

- A security profile shall not remove or weaken any requirement defined in the EUCS scheme.
- A security profile shall not modify the assessment methodology or the assessment methods defined in the EUCS scheme.
- A security profile shall follow the processes defined in the scheme, and shall produce the same deliverables.
- A security profile shall specify the EUCS assurance level that it targets.
- A security profile may define new security controls, or may add new requirements to an existing security control, as long as these requirements do not weaken existing EUCS requirements.
- A security profile may mandate a higher frequency of periodic assessments.
- A security profile may define a dedicated section in the document templates defined in the EUCS scheme.

In order to be recognized in the context of EUCS, Security Profiles shall be published on ENISA's Website, after approval from the ECCG.

A CSP may choose to claim conformity to the requirements of one or several security profiles in addition to the core requirements of the scheme. If this claim is confirmed by the conformity assessment, then the CSP may list the security profile(s) in the certificate documentation.

24.2 FORCE MAJEURE

PROPOSAL

In case of force majeure, a NCCA may take temporary measures to ensure the continuity of certification, by extending the timelines related to the periodic and renewal assessments, by relaxing requirements on the execution of conformity assessment activities, and if necessary, by extending the validity of certificates.

The NCCA shall inform ENISA about the extension and provide transparency on reasons and the duration of extension, and ENISA shall make the information available on their website.

The NCCA shall inform the ECCG about the temporary measures, and if several NCCAs are affected by the same force majeure event, they shall coordinate to ensure that they apply equivalent temporary measures.

24.3 SECURITY OF INFORMATION

PROBLEM STATEMENT

Annex to the EUCSA, item 16: The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

RECOMMENDATION

Unless otherwise provided for in this scheme and without prejudice to existing national provisions and practices in the Member States on confidentiality, all parties¹⁹ involved in the application of this Scheme shall maintain confidentiality and observe professional secrecy with regard to all information and data obtained in carrying out their tasks in order to protect the following:

- a) personal data, in accordance with GDPR²⁰;
- b) commercially sensitive and confidential information and trade secrets of a natural or legal person, including intellectual property rights, during the certification lifecycle of the cloud service and up to the end of the indicated retention time for all certification information, unless disclosure is necessary in the public interest, or subject to court orders;
- c) exchange of information necessary for the effective implementation of this scheme, in particular for the purpose of peer reviews, peer assessments or audits, effective collaboration between the involved authorities and bodies, the handling of publicly unknown and subsequently detected vulnerabilities in the process of, or after certification, and the handling of complaints.

Without prejudice to previous paragraph, information exchanged on a confidential basis between competent authorities and between competent authorities and the Commission shall not be disclosed to the public without the prior agreement of the originating authority.

All information received from the CABs or their subcontractors or the CSPs shall only be used for the purpose of the certification and deemed confidential by the NCCAs – unless a different agreement is reached between the parties or unless an information flow is required by a specific regulation of the scheme.

¹⁹ Including at least the CAB, the NCCA, and their staff, their committees, their subsidiaries, their subcontractors, and any associated body or the staff of external bodies of the CAB or the NCCA.

²⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

All parties involved in the application of this Scheme shall implement security measures in order to ensure the confidentiality of the information provided during the certification process. ENISA may provide guidance on how to insure the security of information based on the workflows associated with the activities described in the EUCS scheme.

RATIONALE

Security of information is key in cybersecurity related activities. All cybersecurity certification related activities fall into the latter.

Information provided by the applicant to the CAB for certification might be sensitive, especially as, the higher the evaluation level, the deeper the evaluator shall go into the analysis of the cloud service and related life-cycle, based on information details that may comprise commercially confidential information and trade secrets, including intellectual property rights.

Information developed by cybersecurity certification activities, such as Assurance Reports, which are associated to vulnerabilities assessment, handling and release, will also contain information sensitive parts that, when poorly protected, may obviously endanger the users of associated cloud services, even when these cloud services are certified.

Therefore, the obligations of the different actors of the scheme to insure the security of information shall be established and take into consideration the requirements for CSPs and developers to comply with Article 55 of the EUCSA, and the necessary respect of Freedom of Information policies and legal frameworks, Access to Information Acts, and/or any other similar national, European and international policies and regulations by any individuals or entities.

24.4 COMPOSITION

PROBLEM STATEMENT

The composition of certificates is not mentioned explicitly in the EUCSA, but it is a common way of building complex certified products or services by leveraging previously certified products and services. In the context of the EUCS scheme, the objective is twofold:

- Allow certified cloud services to be certified along a supply chain.
- Reduce the costs of certifying a cloud service that relies on previously certified products and services by allowing the reuse of evidence and of audit results.

The use of composition leads to specific issues related to the evaluation of composed cloud services, and also to the maintenance of the certification for composed cloud services, relatively to the maintenance of the certification of their components.

RECOMMENDATION

Cloud services are layered systems, in which infrastructure and platform capabilities from a service are often used as a basis for other services. There may also be some dependencies between an application capability and another service. These services used by a CSP in the provision of its own cloud service are referred to as sub-services, supplied by sub-service providers or organizations. The general rules for the consideration of such sub-service providers in the assessment of a cloud service is covered extensively in Annex B: (Meta-approach for the assessment of cloud services). In addition, CSPs need to fulfil specific requirements related to their service providers and suppliers that are defined in Annex A: (Security Objectives and requirements for Cloud Services).

Composition is a particular case, in which the sub-service (then called a base service) is itself a cloud service that has been certified in the EUCS scheme. In such a case the cloud service (or dependent service) relying on the base service can expect the assessment of the requirements related to the base service to be greatly simplified, because they use the same security framework, and because the rules of the scheme (and in particular those related to the CABs) are trusted.

In order to be eligible for composition, the base cloud service shall satisfy some specific requirements, defined in Annex A: (Security Objectives and requirements for Cloud Services), which will allow the assessment of dependent cloud services to be further simplified. These specific requirements consist in defining precisely, in terms of specific EUCS security objectives and requirements, how security responsibilities are split between the base service and the dependent service:

- The base cloud service shall provide a description of their contribution to the EUCS requirement fulfilment of their dependent services, properly justified through references to their own controls; and
- The base service shall provide a list of actionable requirements on Complementary Customer Controls (CCCs, based on the EUCS objectives and requirements) that define the requirements to be fulfilled by the dependent cloud service in order for the base service to fulfil the requirements for EUCS certification at the chosen assurance level.

These two conditions are defined as requirements for base services in Annex A: (Security Objectives and requirements for Cloud Services). Therefore, they are in the scope of the conformity assessment for the base service.

This information can then be used by the CSP of the dependent service in several ways:

- During the design phase, the CSP can use the information about the base service to drive design decisions for its dependent service;
- When building documentation for its certification, the description of the base service's contribution and of its CCCs can be used directly by the CSP of the dependent service, who will simply need to document its implementation of the CCCs; and
- The CAB only needs to verify that this information has not been modified and if necessary that a subset has been properly selected, and will focus on verifying that the CCCs are fulfilled by the dependent service.

In addition, there are a few simple rules that must be followed:

- In order to apply composition, the base service shall be certified at a level equal or greater than the level targeted by the dependent service;
- In order to apply composition fully, the base service shall claim compliance to the security profiles that the dependent service claims compliance to. If the dependent service claims compliance to a security profile that is not claimed by the base service, then this security profile is excluded from the composition, and a classical process shall be used if necessary to demonstrate that the base service satisfies as a subservice the expectations of the dependent service relative to that security profile;
- The dependent service shall add to the requirements to be fulfilled the requirements from the base service's CCCs.
- In its description of its contribution of the base service to the fulfilment of the scheme's requirements, the dependent service shall indicate when the description is the one provided by the base service in its documentation.

Finally, note that:

- A dependent service may use composition with more than one base services;
- Although composition cannot only be applied to base services that have been certified through the EUCS scheme, ENISA will issue with the support of ECCG some guidance about a similar approach for base services that have been assessed through existing National schemes listed in Chapter 16 (Related Schemes), in order to facilitate the transition from National schemes to the EUCS scheme.

25. FURTHER RECOMMENDATIONS

Foreword for Reviewers

The recommendations in this chapter are not intended to be included in the scheme. They are related to the lifecycle of the scheme, specifically measures to be considered between the formal adoption of the scheme and the emission of the first certificates, and measures related to the maintenance of the scheme.

They nevertheless represent important topics that will need to be addressed in order for the scheme to be successful. The scheme adoption topic, in particular, will be of paramount importance for this new scheme, and requires our full attention.

25.1 SCHEME ADOPTION

25.1.1 Problem statement

25.1.1.1 EUCSA Reference

Article 57 1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are not covered by a European cybersecurity certification scheme shall continue to exist.

25.1.1.2 Additional information

The transition period is here considered as the period between the date of adoption of the implementing act adopted pursuant to Article 49(7), and the date established into this implementing act when national schemes shall cease to produce effect.

25.1.2 Recommendation

The EUCS scheme is the first scheme for cloud services at an international level, It will replace at least partly a few existing national schemes, but it is mostly a new scheme that needs to be set up gradually across the European Union.

Prerequisites for scheme adoption

In order for relevant bodies in a Member State to start issuing certificates at the Basic and Substantial levels, the following should happen:

- existing and new CABs get accredited to ISO/IEC 17065, and their internal and external evaluation facilities get accredited to relevant standards;
- the NCCA notifies accredited CABs to the EC;
- CSPs need to get acquainted with the various components of the scheme and update their processes to conform to its requirements;

- CABs need to work with the NCCA to set up monitoring activities; and
- the NCCA sets up the market surveillance process.

In order for the relevant bodies in a Member State to start issuing certificates at level High, the following should also happen:

- the NCCA establishes how High certificates will be issued and take the relevant action (get its CAB-NCCA accredited, and/or designate a CAB for general delegation, and/or organize a prior approval process of certificates); and
- existing and new CABs, including their internal or external evaluation facilities get authorized by the NCCA before notification to the EC;

In addition, before relevant bodies in any Member State can start issuing certificates, the following should happen at European level:

- a maintenance organization is put in place for the EUCS scheme, to further develop the scheme and to support any interpretation and harmonisation question related to the adoption of the new scheme.

The AHWG recommends an adoption period of one (1) year between the adoption of the scheme and the issuance of the first certificate as being technically acceptable.

Scheme adoption and transition period

ENISA may establish associated rules for adopting the scheme as to support the conditions for the scheme to operate. These rules shall be established in cooperation with the ECCG.

For Member States who operate a national scheme for which a transition to the EUCS scheme is required, the transition also needs to be organized to ensure that, after a period of time, only EUCS certificates can be issued. The transition period should allow for:

- termination of current certification projects under the existing schemes, or their easy conversion into EUCS projects;
- smooth transfer of certificates that require maintenance in the long run, therefore under for the EUCS scheme, or reuse for composite evaluations and certifications under the EUCS scheme.

The guiding principles for the transitions are as follows:

- Certificates can be issued by the National scheme at most until the end of the transition period.
- Certificates issued by the National scheme remain valid until the end of their validity period, which cannot be extended.
- The transition to the European scheme is accelerated by defining rules about the reuse of evidence and evaluation results previously used toward the issuance of a National certificate

These rules will be complemented with relevant guidance at the beginning of the transition period, in particular regarding the potential reuse of certificates, evaluation results, and evidence from the national schemes. Such certificates, evaluation results and evidence issued on a given cloud service may be used during the conformity assessment of the same cloud service, or during the conformity assessment of another cloud service for which that cloud service is a subservice.

The AHWG recommends a transition period of one (1) year after the issuance of the first certificates as being technically acceptable.

25.2 SCHEME MAINTENANCE

25.2.1 Problem statement

25.2.1.1 EUCSA Reference

Article 62.4 – The ECCG shall have the following tasks:

e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

25.2.2 Recommendation

The AHWG recommends the following for the maintenance of the EUCS scheme.

The ECCG should mandate groups of experts involving NCCAs, CABs and associated auditors, CSPs and CSCs to:

- improve the security controls and associated requirements;
- improve the assessment methodology and associated documents;
- provide guidance to CABs and CSPs about the prerequisites and operation of the scheme.

The expert groups should focus on methodology harmonization of evaluation activities, analysis of new technologies and vulnerability classes, and propose new or revised supporting documents.

As an alternative, some of the annexes to the scheme, and in particular Annex A: (Security Objectives and requirements for Cloud Services), may be considered for submission to a European Standards Developing Organization (SDO) as a basis for a future European standard, to be referenced in future versions of the EUCS scheme.

The ECCG should define adequate terms of reference for these expert groups. ENISA should publish the list of mandated expert groups and their associated mandates.

26. REFERENCES

STANDARDS AND TECHNICAL SPECIFICATIONS

ISO Standards

- [ISO Supplement] ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedures specific to ISO (in particular, Annex SL)
- [ISO Guide 73] ISO Guide 73:2009, Risk management — Vocabulary
- [ISO9000] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary
- [ISO15408-3] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components
- [ISO17000] ISO/IEC 17000:2020, Conformity assessment – Vocabulary and general principles.
- [ISO17021] ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- [ISO17025] ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories
- [ISO17029] ISO/IEC 17029:2019, Conformity assessment — General principles and requirements for validation and verification bodies
- [ISO17065] ISO/IEC 17065:2012. Conformity assessment — Requirements for bodies certifying products, processes and services
- [ISO17067] ISO/IEC 17067:2013, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes
- [ISO17788] ISO/IEC 17788:2014, Information technology – Cloud computing – Overview and vocabulary.
- [ISO19011] ISO 19011:2018, Guidelines for auditing management systems
- [ISO20000-10] ISO/IEC 20000-10:2019, Information technology – Service management – Part 10: Concepts and vocabulary
- [ISO24765] ISO/IEC/IEEE 24765:2017, Systems and software engineering — Vocabulary
- [ISO27000] ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary.
- [ISO27001] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements
- [ISO27002] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls
- [ISO27005] ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management
- [ISO27006] ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- [ISO27007] ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
- [ISO27017] ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- [ISO27032] ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity
- [ISO29147] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure
- [ISO30111] ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes

International auditing standards

- [IAASB Handbook] 2018 Handbook of international quality control, auditing, review, other assurance, and related service announcements, 2018. ISBN 978-1-60815-389-3.
Available from <https://www.iaasb.org/publications/2018-handbook-international-quality-control-auditing-review-other-assurance-and-related-services-26>
- [ISAE 3000] International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance engagements other than audits or reviews of historical financial information, 2013. In [IAASB Handbook] Vol. 2, pp. 123-206
- [ISAE 3402] International Standard on Assurance Engagements (ISAE) 3402 Assurance reports on controls at a service organization, in [IAASB Handbook], Vol. 2, pp. 217-264
- [ISQC1] International Standard on Quality Control (ISQC), Quality control for firms that perform audits and reviews of financial statements and other assurance and related services engagements. In [IAASB Handbook], Vol 1, pp. 41-75
- [IFAC Ethics] International Ethics Standards Board for Accountants (IESBA) Handbook of the International Code of Ethics for Professional Accountants, 2018. ISBN: 978-1-60815-369-5
Available from: <https://www.ifac.org/system/files/publications/files/IESBA-Handbook-Code-of-Ethics-2018.pdf>

LEGAL TEXTS

- [EUCSA] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019.
- [EC765/2008] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, 2008
- [EU2018/1807] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018.
- [GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.
- [EC1025/2012] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, 2012.
- [Blue Guide] The 'Blue Guide' on the implementation of EU products rules 2016 (Text with EEA relevance) (2016/C 272/01), 2016

OTHER REFERENCES

- [CSP-CERT] CSP-CERT (Cloud Service Provider Certification Working Group), Recommendations for the implementation of the CSP certification scheme, 2019.
Available from: https://drive.google.com/open?id=1J2Njt-mk2iF_ewhPNnhTywpo0zOVcY8J
- [C5] Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloud Computing Compliance Criteria Catalogue (C5), 2020.
Available from: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html
- [SecNumCloud] Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), Référentiel d'exigences pour les prestataires de service d'informatique en nuage (SecNumCloud) v3.1, 2014.
Available from: <https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/>
- [OWASP CA] Open Web Application Security Project (OWASP) Foundation. Component Analysis.
Available from: https://owasp.org/www-community/Component_Analysis

ANNEX A: SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES

PURPOSE	This annex describes the applicable security controls and requirements for all assurance levels.
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 8, Evaluation Methods and Criteria

Foreword for Reviewers

The security controls were initially based on the proposed made by CSP-CERT. However, during and around the fall plenary meeting, a number of issues were brought to our attention regarding these controls under development, including concerns about complexity as well as consistency and clarity issues.

Due to the limited time remaining, the decision was taken to reorganize the security controls and to use the structure and when applicable, the wording of the BSI's C5:2020 criteria, which have the advantage of having been used in practice for quite some time. The criteria have been reorganized into requirements, which have then been assigned to assurance levels. Then, additional sources have been considered, in particular the SecNumCloud scheme, but also relevant standards such as ISO/IEC 27002 and ISO/IEC 27017

There are a few known caveats in this content, including:

- The focus has been on the definition of requirements, so the formulation of the objectives is not as consistent as that of requirements.
- Guidance is not included, except for elements from C5's criteria and SecNumCloud's requirements that have been moved to guidance.

PRINCIPLES

This Annex is an essential component of the scheme, as it defines the technical objectives and requirements that CSPs need to fulfil in order to get a cloud service certified.

Abstraction level

Because this annex is intended to also be an annex to the implementing act for the scheme, it is important to keep a rather high level of abstraction. The objective is here to define whenever possible the requirements in a technology-neutral fashion, and also to avoid mentioning specific technical details which could become outdated very fast.

The requirements defined in this annex shall therefore be complemented by guidance, to be published by ENISA with the support of the ECCG. The requirements in the guidance shall provide the scheme users with a reference way to fulfil the requirements defined in the scheme, typically by providing additional details that describe the required “currently accepted techniques” or “state-of-the-art”.

Most requirements in this annex are written using “shall”, whereas the guidance and a limited number of requirements in this annex are written with “should”. The term “should” is used to indicate recognized means of fulfilling the requirements of the EUCS scheme.

Organization

The requirements are grouped in 19 categories, and each category is divided in a number of themes. Each theme is structured as follows:

- An objective that the requirements aim at achieving.
- Requirements to be met by the controls implemented in support of the certified cloud services, with each requirement associated to an assurance level.
- In some cases, an indication of guidance to be made available, typically when part of a requirement inherited from an existing set of criteria or requirements has been moved to guidance, or when a key concept is expected to be detailed in guidance.

There are many cross-references between requirements and themes. For instance, the ISP-02 theme, which defines how policies and procedures are to be defined, is referenced many times.

Assurance levels

The requirements defined in the present Annex are labelled Basic, Substantial or High:

- Requirements labelled Basic apply to all assurance levels.
- Requirements labelled Substantial apply to levels Substantial and High, and they will in most cases be considered as guidance for level Basic (*i.e.*, the reference method to achieve the Basic requirements, which are often less detailed).
- Requirements labelled High only apply to level High.

Typically, the requirements corresponding to an objective are organized as follows:

- Basic requirements define a baseline, often with limited details or constraints
- Substantial requirements add to that baseline further details and constraints. Sometimes, there are a few specific Substantial requirements.
- High requirements add further constraints. Some are also related to continuous monitoring, or to additional testing and review requirements, contributing to an increase in the depth of the audit.

Continuous monitoring

The requirements related to continuous monitoring typically mention “automated monitoring” or “automatically monitor” in their text. The intended meaning of “monitor automatically” is:

1. Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;
2. Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;
3. Report deviations to subject matter experts who can analyse the deviations in a timely manner;
4. If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and
5. If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.

These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity. Nevertheless, the introduction of continuous auditing, at least for level High, remains a mid- or long-term objective, and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.

Further guidance will be provided about acceptable mechanisms and processes.

A.1 ORGANISATION OF INFORMATION SECURITY

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

OIS-01 INFORMATION SECURITY MANAGEMENT SYSTEM

Objective

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

Requirements

Ref	Description	Ass. Level
OIS-01.1	The CSP shall define, implement, maintain and continually improve an information security management system (ISMS), covering at least the operational units, locations and processes for providing the cloud service	Basic
OIS-01.2	The ISMS shall be in accordance to ISO/IEC 27001	Substantial
OIS-01.3	The ISMS shall have a valid certification according to ISO/IEC 27001 or to national schemes based on ISO 27001	High
OIS-01.4	The CSP shall document the measures for documenting, implementing, maintaining and continuously improving the ISMS	Basic
OIS-01.5	The documentation shall include at least: <ul style="list-style-type: none"> • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3). 	Substantial

OIS-02 SEGREGATION OF DUTIES

Objective

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

Requirements

Ref	Description	Ass. Level
OIS-02.1	The CSP shall perform a risk assessment as defined in RM-01 about the accumulation of responsibilities or tasks on roles or individuals, regarding the provision of the cloud service	Basic
OIS-02.2	The risk assessment shall cover at least the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the CSP: <ul style="list-style-type: none"> • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IAM-01); • Development, testing and release of changes (cf. DEV-01, CCM-01); and • Operation of the system components. 	Basic
OIS-02.3	The CSP shall implement the mitigating measures defined in the risk assessment, privileging separation of duties, unless impossible for organisational or technical reasons, in which case the measures shall include the monitoring of activities in order to detect unauthorised or unintended changes as well as misuse and the subsequent appropriate actions	Basic

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

OIS-03 CONTACT WITH AUTHORITIES AND INTEREST GROUPS

Objective

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

Requirements

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

OIS-04 INFORMATION SECURITY IN PROJECT MANAGEMENT

Objective

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

Requirements

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

A.2 INFORMATION SECURITY POLICIES

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

ISP-01 GLOBAL INFORMATION SECURITY POLICY

Objective

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

Requirements

Ref	Description	Ass. Level
ISP-01.1	The CSP shall document a global information security policy covering at least the following aspects: <ul style="list-style-type: none"> the importance of information security, based on the requirements of cloud customers in relation to information security, as well as on the need to ensure the security of the information processed and stored by the CSP and the assets that support the services provided the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; the commitment of the CSP to implement the security measures required to achieve the established security objectives. the most important aspects of the security strategy to achieve the security objectives set; and the organisational structure for information security in the ISMS application area. 	Basic
ISP-01.2	The CSP's top management shall approve and endorse the global information security policy	Basic
ISP-01.3	The CSP shall review the global information security policy at least following any significant organizational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management	Substantial
ISP-01.4	The CSP shall review the global information security policy at least annually	High
ISP-01.5	The CSP shall communicate and make available the global information security policy to internal and external employees and to cloud service customers	Basic

ISP-02 SECURITY POLICIES AND PROCEDURES

Objective

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

Requirements

Ref	Description	Ass. Level
ISP-02.1	The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including at least the following aspects: <ul style="list-style-type: none"> Objectives; Scope; Roles and responsibilities within the organization; Roles and dependencies on other organisations (especially cloud customers and subservice organisations); Steps for the execution of the security strategy; and Applicable legal and regulatory requirements. 	Basic

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

Guidance elements	
ISP-02.1	Add in the guidance the list of requirements that mention policies and procedures, once Annex A is complete.
ISP-02.6	The review of policies and procedures should consider at least the following aspects: <ul style="list-style-type: none"> Organisational and technical changes in the procedures for providing the cloud service; and Legal and regulatory changes in the CSP's environment.

ISP-03 EXCEPTIONS

Objective

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

Requirements

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

A.3 RISK MANAGEMENT

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

RM-01 RISK MANAGEMENT POLICY

Objective

Risk management policies and procedures are documented and communicated to stakeholders

Reference: [ISO27005]

Requirements

Ref	Description	Ass. Level
RM-01.1	The CSP shall document policies and procedures in accordance with ISP-02 for the following aspects: <ul style="list-style-type: none"> • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; • Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results. 	Basic
RM-01.2	The CSP shall use a documented risk analysis method that guarantees reproducibility and comparability of the approach	Substantial

Guidance elements

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

RM-02 RISK ASSESSMENT IMPLEMENTATION

Objective

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

Requirements

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

Guidance elements	
RM-02.1	<p>The scope of risk identification should include the aspects below, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider:</p> <ul style="list-style-type: none"> • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; • Occurrence of weak points and malfunctions in the integration at system level of technical protective measures; • Attacks via access points, including interfaces accessible from public networks (in particular administrative interfaces); • Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and • Dependencies on subservice organisations.
RM-02.1	<p>For higher assurance levels, specific technical risks should be considered, including:</p> <ul style="list-style-type: none"> • The risks of failure of the mechanisms of partitioning technical infrastructure resources (memory, calculation, storage, network) that are shared between clients; and • The risks linked to the incomplete or non-secure erasing of data stored in the memory areas or of storage shared between clients, in particular during reallocations of memory and storage areas.

RM-03 RISK TREATMENT IMPLEMENTATION

Objective

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

Requirements

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

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

A.4 HUMAN RESOURCES

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

HR-01 HUMAN RESOURCE POLICIES

Objective

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

Requirements

Ref	Description	Ass. Level
HR-01.1	The CSP shall classify information security-sensitive positions according to their level of risk, including positions related to IT administration and to the provisioning of the cloud service in the production environment, and all positions with access to cloud customer data or system components.	Basic
HR-01.2	The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement from internal and external employees to act ethically in their professional duties.	Basic
HR-01.3	The CSP shall document, communicate and implement a policy that describes actions to take in the event of violations of policies and instructions or applicable legal and regulatory requirements, including at least the following aspects: <ul style="list-style-type: none"> • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact 	Basic
HR-01.4	If disciplinary measures are defined in the policy mentioned in HR-01.3, then the internal and external employees of the CSP shall be informed about possible disciplinary measures and the use of these disciplinary measures shall be appropriately documented.	Basic

Guidance elements	
HR-01.2	The agreement should at least stipulate that for any matter related to the security of the cloud service: <ul style="list-style-type: none"> • professional duties are performed with loyalty, discretion and impartiality; and • Internal and external employees use only those methods, tools and techniques that have been approved by the Cloud Service Provider.
HR-01.2	The Code of Ethics should also consider the following provisions, especially at higher levels: <ul style="list-style-type: none"> • employees pledge to not disclose information to a third party, even if anonymised and decontextualised, which has been obtained or generated as part of the service, unless the Cloud Service Customer has given formal written authorisation; • employees pledge to alert the service provider to all clearly illegal content discovered during the provision of the service; and • employees pledge to comply with the legislation and regulations in force and with best practices related to their activities.

HR-02 VERIFICATION OF QUALIFICATION AND TRUSTWORTHINESS

Objective

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

Requirements

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

Guidance elements		
HR-02.1:	<p>The agreement should at least stipulate that for any matter related to the security of the cloud service:</p> <ul style="list-style-type: none"> • professional duties are performed with loyalty, discretion and impartiality; and • Internal and external employees use only those methods, tools and techniques that have been approved by the CSP. <p>For higher levels, the following areas should also be included:</p> <ul style="list-style-type: none"> • Request of a police clearance certificate for applicants; and • Evaluation of the risk to be blackmailed. 	

HR-03 EMPLOYEE TERMS AND CONDITIONS

Objective

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

Requirements

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

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

HR-04 SECURITY AWARENESS AND TRAINING

Objective

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

Requirements

Ref	Description	Ass. Level
HR-04.1	The CSP shall define a security awareness and training program that covers the following aspects: <ul style="list-style-type: none"> • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents. 	Basic
HR-04.2	The CSP shall define an awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties	Substantial
HR-04.3	The CSP shall review their security awareness and training program based on changes to policies and instructions and the current threat situation	Basic
HR-04.4	The CSP shall update their security awareness and training program at least annually	Substantial
HR-04.5	The CSP shall ensure that all employees complete the security awareness and training program defined for them	Basic
HR-04.6	The CSP shall ensure that all employees complete the security awareness and training program on a regular basis, and when changing target group	Substantial
HR-04.7	The CSP shall automatically monitor the completion of the security awareness and training program	High
HR-04.8	The CSP shall measure and evaluate the learning outcomes achieved through the awareness and training programme	Substantial
HR-04.9	The CSP shall measure and evaluate in a target group-oriented manner the learning outcomes achieved through the awareness and training programme. The measurements shall cover quantitative and qualitative aspects, and the results shall be used to improve the awareness and training programme.	High
HR-04.10	The CSP shall verify the effectiveness of the security awareness and training program using practical exercises in security awareness training that simulate actual cyber-attacks	Substantial

HR-05 TERMINATION OR CHANGE IN EMPLOYMENT

Objective

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

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

Requirements

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

HR-06 CONFIDENTIALITY AGREEMENTS

Objective

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

Requirements

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

A.5 ASSET MANAGEMENT

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

AM-01 ASSET INVENTORY

Objective

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

Requirements

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

Guidance elements	
AM-01.1	The assets include the physical and virtual objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility, e.g. firewalls, load balancers, web servers, application servers and database servers.
AM-01.3	The information recorded should include: <ul style="list-style-type: none"> the information for identifying the asset the function of the asset; the model and version of the asset; the location of the asset;
AM-01.3	The CSP shall log at least all changes to the information related to risk management on each asset

AM-02 ACCEPTABLE USE AND SAFE HANDLING OF ASSETS POLICY

Objective

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

Requirements

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

Guidance elements		
AM-02.1	<p>The policies and procedures for acceptable use and safe handling of assets shall address at least the following aspects of the asset lifecycle as applicable to the asset:</p> <ul style="list-style-type: none"> • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components; • Inventory; • Classification and labelling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support, and security patches are not available anymore; • Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning. 	
AM-02.3	<p>Definition from NIST's CSRC: Portable data storage medium that can be added to or removed from a computing device or network.</p> <p>Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).</p>	

AM-03 COMMISSIONING AND DECOMMISSIONING OF HARDWARE

Objective

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

Requirements

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

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

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

Objective

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

Any assets handed over are returned upon termination of employment.

Requirements

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

AM-05 ASSET CLASSIFICATION AND LABELLING

Objective

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

Requirements

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

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

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

A.6 PHYSICAL SECURITY

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

PS-01 PHYSICAL SECURITY PERIMETERS

Objective

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

Requirements

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

PS-02 PHYSICAL SITE ACCESS CONTROL

Objective

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

Requirements

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

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

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

PS-03 WORKING IN NON-PUBLIC AREAS

Objective

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

Requirements

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

PS-04 EQUIPMENT PROTECTION

Objective

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

Requirements

Ref	Description	Ass. Level
PS-04.1	The CSP shall document, communicate, and implement policies and procedures concerning the protection of equipment and including at least the following aspects: <ul style="list-style-type: none"> Protecting power and communications cabling from interception, interference or damage; Protecting equipment during maintenance operations; Protecting equipment holding customer data during transport. 	Basic
PS-04.2	The procedures defined in PS-04.1 shall include a procedure to check the protection of power and communications cabling, to be performed regularly, at least every two years, as well as in case of suspected manipulation by qualified personnel	Substantial
PS-04.3	The policies and procedures in PS-04.1 shall include a procedure for transferring any equipment containing customer data off-site for disposal that guarantees that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site	Substantial
PS-04.4	The procedure mentioned in PS-04.3 shall include a formal validation by top management of the CSP or by the authorized body that validated this procedure	High
PS-04.4	The CSP shall establish a wiring scheme and keep it up-to-date	High
PS-04.5	The CSP shall ensure that the maintenance agreements for equipment used to host the cloud service make it possible to have security updates installed timely on this equipment	High
PS-04.6	The policies and procedures in PS-04.1 shall include measures to ensure that the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) are compatible with the cloud service’s availability and security requirements	High
PS-04.7	The CSP shall ensure that an equipment containing a media with customer data can be returned to a third party only if the customer data stored on it is encrypted in accordance with CKM-03 or has been destroyed beforehand using a secure deletion mechanism	High
PS-04.8	The CSP shall use encryption on the removable media and the backup media intended to move between security areas according to the sensitivity of the data stored on the media	Basic

Guidance elements	
PS-04.2	The checks to be performed should include at least the following aspects: <ul style="list-style-type: none"> Traces of violent attempts to open closed distributors; Up-to-datedness of the documentation in the distribution list; Conformity of the actual wiring and patching with the documentation; The short-circuits and earthing of unneeded cables are intact; and Impermissible installations and modifications.

PS-05 PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

Objective

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

Requirements

Ref	Description	Ass. Level
PS-05.1	<p>The CSP shall document and communicate a set of security requirements related to external and environmental threats in a policy according to SP-02, addressing the following risks in accordance with the applicable legal and contractual requirements:</p> <ul style="list-style-type: none"> • Faults in planning; • Unauthorised access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. 	Basic
PS-05.2	The security requirements defined in PS-05.1 for datacentres shall be based on criteria which comply with established rules of technology	Substantial
PS-05.3	The security requirements defined in PS-05.1 for datacentres shall include time constraints for self-sufficient operation in the event of exceptional events and maximum tolerable utility downtime	High
PS-05.4	The security requirements defined in PS-05.1 for datacentres shall include tests of physical protection and detection equipment, to be performed at least annually	High
PS-05.5	The CSP shall provide the cloud service from at least two locations that are separated by an adequate distance and that provide each other with operational redundancy or resilience	Substantial
PS-05.6	The CSP shall check the effectiveness of the redundancy at least once a year by suitable tests and exercises (cf. BCM-04)	Substantial

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

A.7 OPERATIONAL SECURITY

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

OPS-01 CAPACITY MANAGEMENT – PLANNING

Objective

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

Requirements

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

OPS-02 CAPACITY MANAGEMENT – MONITORING

Objective

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

Requirements

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

OPS-03 CAPACITY MANAGEMENT – CONTROLLING OF RESOURCES

Objective

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

Requirements

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

OPS-04 PROTECTION AGAINST MALWARE – POLICIES

Objective

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

Requirements

Ref	Description	Ass. Level
OPS-04.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects: <ul style="list-style-type: none"> • Use of system-specific protection mechanisms; • Operating protection programs on system components under the responsibility of the CSP that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment. 	Basic
OPS-04.2	The CSP shall create regular reports on the malware checks performed, which shall be reviewed and analysed by authorized bodies in the reviews of the policies related to malware	Substantial
OPS-04.3	The policies and instructions related to malware shall include the technical measures taken to securely configure, protect from malware, and monitor the administration interfaces (both the customer's self-service and the CSP's administration)	High
OPS-04.4	The CSP shall update the anti-malware products at the highest frequency that the vendors actually offer	High

OPS-05 PROTECTION AGAINST MALWARE – IMPLEMENTATION

Objective

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

Requirements

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

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

OPS-06 DATA BACKUP AND RECOVERY – POLICIES

Objective

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

Requirements

Ref	Description	Ass. Level
OPS-06.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for data backup and recovery	Basic
OPS-06.2	The policies and procedures for backup and recovery shall cover at least the following aspects: <ul style="list-style-type: none"> The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); Data is backed up in encrypted, state-of-the-art form; Access to the backed-up data and the execution of restores is performed only by authorised persons; and Tests of recovery procedures (cf. OPS-08). 	Substantial

OPS-07 DATA BACKUP AND RECOVERY – MONITORING

Objective

The proper execution of data backups is monitored.

Requirements

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

OPS-08 DATA BACKUP AND RECOVERY – REGULAR TESTING

Objective

The proper restoration of data backups is regularly tested.

Requirements

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

OPS-09 DATA BACKUP AND RECOVERY – STORAGE

Objective

Backup data is stored at an appropriately remote location.

Requirements

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

OPS-10 LOGGING AND MONITORING – POLICIES

Objective

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

Requirements

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

Ref	Description	Ass. Level
	<ul style="list-style-type: none"> • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs; • Define roles and responsibilities for setting up and monitoring logging; • Time synchronisation of system components; and • Compliance with legal and regulatory frameworks. 	

OPS-11 LOGGING AND MONITORING – DERIVED DATA MANAGEMENT

Objective

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

Requirements

Ref	Description	Ass. Level
OPS-11.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 that govern the secure handling of derived data	Basic
OPS-11.2	The policies and procedures on derived data shall cover at least the following aspects: <ul style="list-style-type: none"> • Purpose for the collection and use of derived data beyond the operation of the cloud service, including purposes related to the implementation of security controls; • Anonymisation of the data whenever used in a context that goes beyond a single CSC; • Period of storage reasonably related to the purposes of the collection; • Guarantees of deletion when the purposes of the collection are fulfilled and further storage is no longer necessary; and • Provision of the derived data to CSCs according to contractual agreements. 	Substantial
OPS-11.3	The CSP shall list in the contractual agreement with the CSC all purposes for the collection of use of derived data that are not related to the implementation of security controls or to billing	Substantial
OPS-11.4	Derived data, including log data, shall be taken into consideration in regulatory compliance assessments.	High

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

OPS-12 LOGGING AND MONITORING – IDENTIFICATION OF EVENTS

Objective

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

Requirements

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

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

Objective

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

Requirements

Ref	Description	Ass. Level
OPS-13.1	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation	Basic
OPS-13.2	Log data shall be deleted when it is no longer required for the purpose for which they were collected	Basic
OPS-13.3	The communication between the assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality	Basic
OPS-13.4	The communication between the assets to be logged and the logging servers shall be encrypted using state-of-the-art encryption or shall take place on a dedicated administration network	Substantial
OPS-12.5	The CSP shall implement technically supported procedures to fulfil requirements related to the access, storage and deletion related to the following restrictions: <ul style="list-style-type: none"> • Access only to authorised users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection. 	Substantial
OPS-13.6	The CSP shall provide CSCs, upon request, access to customer-specific logging through an API. The logging shall comply with the CSP's protection requirements, including logical or physical separation of log and customer data	High
OPS-13.7	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data to fulfil OPS-13.2	High

Guidance elements

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

OPS-14 LOGGING AND MONITORING – ATTRIBUTION

Objective

Log data can be unambiguously attributed to a CSC.

Requirements

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

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

OPS-15 LOGGING AND MONITORING – CONFIGURATION

Objective

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

Requirements

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

OPS-16 LOGGING AND MONITORING – AVAILABILITY

Objective

Systems for logging and monitoring are themselves monitored for availability.

Requirements

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

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

OPS-17 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES

Objective

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

Requirements

Ref	Description	Ass. Level
OPS-17.1	The CSP shall document, communicated and implement in accordance to ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service	Basic
OPS-17.2	The policies and procedures shall describe measures regarding at least the following aspects: <ul style="list-style-type: none"> Regular identification of vulnerabilities; Assessment of the severity of identified vulnerabilities; Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities. 	Substantial
OPS-17.3	The CSP shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities	Basic
OPS-17.4	The CSP shall mandate in its policies and procedures the immediate handling of “critical” vulnerabilities and the handling of “high” vulnerabilities within a day, with a follow-up of the vulnerability until it has been remediated	Substantial

Guidance elements		
OPS-17.3	The requirement stops short of requiring the use of CVSS, although the CSP is encouraged to use a version of CVSS. As a rule of thumb: <ul style="list-style-type: none"> A critical vulnerability would correspond to CVSS scores between 9.0 and 10.0 A high vulnerability would correspond to CVSS scores between 7.0 and 8.9 	
OPS-17.4	A critical vulnerability is expected to be handled within a few hours, and the EUCS scheme requires the CSP to notify its CAB of such a vulnerability.	

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

Objective

Online registers are used to identify and publish known vulnerabilities.

Requirements

Ref	Description	Ass. Level
OPS-18.1	The CSP shall publish and maintain a publicly and easily accessible online register of known vulnerabilities that affect the cloud service and assets provided by the CSP that the CSCs have to install or operate under their own responsibility	Basic
OPS-18.2	The online register shall indicate at least the following information for every vulnerability: <ul style="list-style-type: none"> • A presentation of the vulnerability following an industry-accepted scoring system; • A description of the remediation options for that vulnerability; • Information on the availability of updates or patches for that vulnerability; • Information about the remediation or deployment of patches or updates by the CSP or CSC, including detailed instructions for operations to be performed by the CSC. 	Basic
OPS-18.3	The CSP shall publish and maintain a list of pointers to online registers published by its subservice providers and suppliers, or integrate regularly the content of these online registers relevant to the cloud service into its own online register (cf. OPS-18.1)	Basic
OPS-18.4	The CSP shall consult regularly the online registers published by its subservice providers and suppliers, analyse the potential impact of the published vulnerabilities on the cloud service, and handle them according to the vulnerability handling process (cf. OPS-17)	Basic
OPS-18.5	The CSP shall consult the online registers published by its subservice providers and suppliers at least daily, and update accordingly its own online register	Substantial
OPS-18.6	The CSP shall equip with automatic update mechanisms the assets provided by the CSP that the CSCs have to install or operate under their own responsibility, to ease the rollout of patches and updates after an initial approval from the CSC	High

Guidance elements

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

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

Objective

Tests are performed on a regular basis to identify vulnerabilities.

Requirements

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

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

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

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

Objective

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

Requirements

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

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

Objective

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

Requirements

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

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

OPS-22 SEPARATION OF DATASETS IN THE CLOUD INFRASTRUCTURE

Objective

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

Requirements

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

A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT

Limit access to information and information processing facilities

IAM-01 POLICIES FOR ACCESS CONTROL TO INFORMATION

Objective

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

Requirements

Ref	Description	Ass. Level
IAM-01.1	The CSP shall document, communicate and make available role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on the business and security requirements of the CSP, in which at least the following aspects are covered: <ul style="list-style-type: none"> Parameters to be considered for making access control decisions Granting and modifying access rights based on the “least-privilege” principle and on the “need-to-know” principle. Use of a role-based mechanism for the assignment of access rights Segregation of duties between managing, approving and assigning access rights Dedicated rules for users with privileged access Requirements for the approval and documentation of the management of access rights 	Basic
IAM-01.2	The CSP shall link the access control policy defined in IAM-01.1 with the physical access control policy defined in PS-02.1, to guarantee that the access to the premises where information is located is also controlled.	Basic
IAM-01.3	The CSP shall base its access control policy on the use of role-based access control.	Substantial

IAM-02 MANAGEMENT OF USER ACCOUNTS

Objective

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

Requirements

Ref	Description	Ass. Level
IAM-02.1	The CSP shall document policies for managing accounts, according to ISP-02, in which at least the following aspects are described: <ul style="list-style-type: none"> Assignment of unique usernames Definition of the different types of accounts supported, and assignment of access control parameters and roles to be considered for each type Events leading to blocking and revoking accounts 	Basic
IAM-02.2	The CSP shall document, communicate and make available policies for managing accounts of users under the responsibility of the CSP, according to ISP-02 and extending the policies defined in IAM-02.1, in which at least the following aspects are described: <ul style="list-style-type: none"> Segregation of duties between managing, approving and assigning user accounts Regular review of assigned user accounts and associated access rights 	Substantial

Ref	Description	Ass. Level
	<ul style="list-style-type: none"> Blocking and revoking accounts in the event of inactivity or potential account compromise Requirements for the approval and documentation of the management of user accounts 	
IAM-02.3	<p>The CSP shall document, communicate and make available policies for managing accounts of users under the responsibility of the CSCs, according to ISP-02 and extending the policies defined in IAM-02.1, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> Access control mechanisms available to CSCs Access control parameters that the CSC is allowed to configure 	Substantial
IAM-02.4	The CSP shall document and implement procedures for managing personal user accounts and access rights to internal and external employees that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.5	The CSP shall document and implement procedures for managing non-personal shared accounts and associated access rights that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.6	The CSP shall document and implement procedures for managing technical accounts and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights concept and with the policies for managing accounts	Basic
IAM-02.7	The CSP shall offer CSCs a self-service with which they can independently manage user accounts for all users under their responsibility.	Substantial
IAM-02.8	The CSP shall be able to provide, for a given user account, whether it falls under the responsibility of the CSP or of the CSC, as well as the list of the access rights granted to that account.	High

IAM-03 LOCKING, UNLOCKING AND REVOCATION OF USER ACCOUNTS

Objective

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

Requirements

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

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

IAM-04 MANAGEMENT OF ACCESS RIGHTS

Objective

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

Requirements

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

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

IAM-05 REGULAR REVIEW OF ACCESS RIGHTS

Objective

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

Requirements

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

IAM-06 PRIVILEGED ACCESS RIGHTS

Objective

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

Requirements

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

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

Guidance elements		
IAM-06.4	Shared account are typically privileged; they should also be assigned to more than one employee	
IAM-06.7 IAM-06.8	The notion of “strong authentication” will need to be described in the guidance, along the lines of: <ul style="list-style-type: none"> • for human users, two-factor or multi-factor authentication; and • for non-human users, authentication using a cryptographic mechanism that satisfies the requirements in CKM-01. 	

IAM-07 AUTHENTICATION MECHANISMS

Objective

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

Requirements

Ref	Description	Ass. Level
IAM-07.1	The CSP shall document and implement a policy and procedures about authentication mechanisms, covering at least the following aspects: <ul style="list-style-type: none"> • The selection of mechanisms suitable for every type of account and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new accounts; • Rules for the renewal of credentials, including periodic renewals, renewals in case of loss or compromise; and • Rules on the required strength of credentials, together with mechanisms to communicate and enforce the rules; 	Basic
IAM-07.2	The access to all environments of the CSP shall be authenticated, including non-production environments	Substantial
IAM-07.3	The access to the production environment of the CSP shall require strong authentication	High
IAM-07.4	The access to all environments of the CSP containing CSC data shall require strong authentication	High
IAM-07.5	Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security	Substantial
IAM-07.6	For access to non-personal shared accounts, the CSP shall implement measures that require the users to be authenticated with their personal account before being able to access these technical accounts	Substantial
IAM-07.7	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts	Basic

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

IAM-08 PROTECTION AND STRENGTH OF CREDENTIALS

Objective

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

Requirements

Ref	Description	Ass. Level
IAM-08.1	The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: <ul style="list-style-type: none"> • Non-reuse of credentials • Trade-offs between entropy and ability to memorize • Recommendations for renewal of passwords • Rules on storage of passwords 	Basic
IAM-08.2	The CSP rules and recommendations defined in IAM-08.1 shall address at least the following aspects: <ul style="list-style-type: none"> • Recommendations on password managers • Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling 	Substantial
IAM-08.3	The CSP shall require users to whom authentication credentials are provided to sign a declaration in which they assure that they treat personal (or shared) authentication confidentially and keep it exclusively for themselves	High
IAM-08.4	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01)	Basic
IAM-08.5	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	Basic
IAM-08.6	When creating credentials, compliance with specifications is enforced automatically as far as technically possible	Substantial
IAM-08.7	When a credential associated to a personal account is changed or renewed, the person associated to that account shall be notified	Substantial
IAM-08.8	Any password communicated to a user through e-mail, message or similar shall be changed by the user after its first use, and its validity shall not exceed 14 days after communication to the user	Substantial
IAM-08.9	The CSP shall make available to the CSC the rules and recommendations that shall or may apply to the users under their responsibility, and provide the CSC with tools to manage and enforce these rules	Substantial

IAM-09 GENERAL ACCESS RESTRICTIONS

Objective

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

Requirements

Ref	Description	Ass. Level
IAM-09.1	The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems	Basic
IAM-09.2	The CSP shall design, develop, configure and deploy the information system providing the cloud service to include a partitioning between the technical infrastructure and the equipment required for the administration of the cloud service and the assets it hosts	Substantial
IAM-09.3	The CSP shall separate the administration interfaces made available to CSCs from those made available to its internal and external employees, and in particular: <ul style="list-style-type: none"> The administration accounts under the responsibility of the CSP shall be managed using tools and directories that are separate from those used for the management of user accounts under the responsibility of the CSCs; The administration interfaces made available to CSCs shall not allow for any connection from accounts under the responsibility of the CSP; The administration interfaces used by the CSP shall not be accessible from the public network and as such shall not allow for any connection from accounts under the responsibility of the CSC. 	High
IAM-09.4	The CSP shall implement suitable measures for partitioning between the CSCs	Basic
IAM-09.5	The CSP shall timely inform a CSC whenever internal or external employees of the CSP access in a non-encrypted form to the CSC's data processed, stored or transmitted in the cloud service without the prior consent of the CSC, including at least: <ul style="list-style-type: none"> Cause, time, duration, type and scope of the access; Enough details to enable subject matters experts of the CSC to assess the risks of the access. 	Substantial
IAM-09.6	The CSP shall require prior consent from a CSC before any access in a non-encrypted form to the CSC's data processed, stored or transmitted in the cloud service, providing meaningful information as defined in IAM-09.5.	High
IAM-09.7	If the CSP offers to its CSCs interfaces for administrators and for end users, these interfaces shall be separated	Substantial

Guidance elements

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

A.9 CRYPTOGRAPHY AND KEY MANAGEMENT

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

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

Objective

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

Requirements

Ref	Description	Ass. Level
CKM-01.1	The CSP shall document, communicate, make available and implement policies with technical and organizational safeguards for encryption and key management, according to ISP-02, in which at least the following aspects are described: <ul style="list-style-type: none"> • Usage of strong encryption procedures and secure network protocols • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys • Consideration of relevant legal and regulatory obligations and requirements 	Basic
CKM-01.2	Cryptography policies and procedures shall include risk-based provisions for the use of encryption aligned with the data classification schemes and considering the communication channel, type, strength and quality of the encryption	Substantial
CKM-01.3	The strong encryption procedures and secure network protocols mentioned in the cryptography policies and procedures shall correspond to the state-of-the-art	Substantial

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

CKM-02 ENCRYPTION OF DATA IN TRANSIT

Objective

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

Requirements

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

CKM-03 ENCRYPTION OF DATA AT REST

Objective

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

Requirements

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

CKM-04 SECURE KEY MANAGEMENT

Objective

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

Requirements

Ref	Description	Ass. Level
CKM-04.1	Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects: <ul style="list-style-type: none"> • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; • Handling of compromised keys; and • Withdrawal and deletion of keys; 	Basic
CKM-04.2	For the secure storage of keys, the key management system shall be separated from the application and middleware levels	Substantial
CKM-04.3	For the secure storage of keys and other secrets used for the administration tasks, the CSP shall use a suitable security container, software or hardware	High
CKM-04.4	If pre-shared keys are used, the specific provisions relating to the secure use of this procedure shall be specified separately.	Substantial

A.10 COMMUNICATION SECURITY

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

CS-01 TECHNICAL SAFEGUARDS

Objective

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

Requirements

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

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

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

Objective

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

Requirements

Ref	Description	Ass. Level
CS-02-1	<p>The CSP shall document, communicate, make available and implement specific security requirements to connect within its network, including at least:</p> <ul style="list-style-type: none"> when the security zones are to be separated and when the cloud customers are to be logically or physically segregated; what communication relationships and what network and application protocols are permitted in each case; how the data traffic for administration and monitoring are segregated from each other at the network level; what internal, cross-location communication is permitted; and what cross-network communication is allowed. 	Basic

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

Objective

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

Requirements

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

CS-04 CROSS-NETWORK ACCESS

Objective

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

Requirements

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

CS-05 NETWORKS FOR ADMINISTRATION

Objective

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

Requirements

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

CS-06 TRAFFIC SEGREGATION IN SHARED NETWORK ENVIRONMENTS

Objective

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

Requirements

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

Guidance elements

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

CS-07 NETWORK TOPOLOGY DOCUMENTATION

Objective

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

Requirements

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

CS-08 SOFTWARE DEFINED NETWORKING

Objective

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

Requirements

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

CS-09 DATA TRANSMISSION POLICIES

Objective

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

Requirements

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

A.11 PORTABILITY AND INTEROPERABILITY

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

PI-01 DOCUMENTATION AND SECURITY OF INPUT AND OUTPUT INTERFACES

Objective

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

Requirements

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

Guidance elements

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

PI-02 CONTRACTUAL AGREEMENTS FOR THE PROVISION OF DATA

Objective

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

Requirements

Ref	Description	Ass. Level
PI-02.1	<p>The CSP shall include in cloud service contractual agreements, at least, the following aspects concerning the termination of the contractual relationship:</p> <ul style="list-style-type: none"> • Type, scope and format of the data the CSP provides to the CSC; • Delivery methods of the data to the cloud customer; • Definition of the timeframe, within which the CSP makes the data available to the CSC; • Definition of the point in time as of which the CSP makes the data inaccessible to the CSC and deletes these; and • The CSC's responsibilities and obligations to cooperate for the provision of the data. 	Basic

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

PI-03 SECURE DELETION OF DATA

Objective

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

Requirements

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

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

A.12 CHANGE AND CONFIGURATION MANAGEMENT

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

CCM-01 POLICIES FOR CHANGES TO INFORMATION SYSTEMS

Objective

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

Requirements

Ref	Description	Ass. Level
CCM-01.1	The CSP shall document, implement, and communicate policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02	Basic
CCM-01.2	The change management policies and procedures shall cover at least the following aspects: <ul style="list-style-type: none"> • Criteria for risk assessment, categorization and prioritization of changes and related requirements for the type and scope of testing to be performed, and necessary approvals; • Requirements for the performance and documentation of tests; • Requirements for segregation of duties during planning, testing, and release of changes; • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; • Requirements for the documentation of changes in the system, operational and user documentation; and • Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes. 	Substantial

CCM-02 RISK ASSESSMENT, CATEGORISATION AND PRIORITISATION OF CHANGES

Objective

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

Requirements

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

CCM-03 TESTING CHANGES

Objective

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

Requirements

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

Guidance elements

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

CCM-04 APPROVALS FOR PROVISION IN THE PRODUCTION ENVIRONMENT

Objective

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

Requirements

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

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

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

CCM-05 PERFORMING AND LOGGING CHANGES

Objective

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

Requirements

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

CCM-06 VERSION CONTROL

Objective

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

Requirements

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

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

A.13 DEVELOPMENT OF INFORMATION SYSTEMS

Ensure information security in the development cycle of information systems

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

Objective

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

Requirements

Ref	Description	Ass. Level
DEV-01.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 with technical and organisational measures for the secure development of the cloud service.	Basic
DEV-01.2	The policies and procedures for secure development shall consider information security from the earliest phases of design	Basic
DEV-01.3	The policies and procedures for secure development shall be based on recognised standards and methods with regard to the following aspects: <ul style="list-style-type: none"> • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); • Security in operation (reaction to identified faults and vulnerabilities); and • Secure coding standards and practices (avoiding the introduction of vulnerabilities in code). 	Substantial
DEV-01.4	The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools	Substantial

Guidance elements

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

DEV-02 DEVELOPMENT SUPPLY CHAIN SECURITY

Objective

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

Requirements

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

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

Guidance elements		
DEV-02.1	For its software components, the list of dependencies is often called Software Board of Materials (SBoM). In the context of [EUCSA], Article 51(d) requires the identification and documentation of known dependencies. Dependencies should include all software modules, libraries or APIs used, as well as development tools.	
DEV-02.2	The policy should cover the following aspects: <ul style="list-style-type: none"> • Restrictions on component age; • Restrictions on outdated and EOL/EOS components; • Restrictions on components with known vulnerabilities; • Restrictions on public repository usage; • Restrictions on acceptable licenses; • Component update requirements; • Deny list of prohibited components and versions; and • Acceptable community contribution guidelines. This list is inspired from the OWASP requirements on open source software [OWASP CA].	
DEV-02.4	The use of certified products may considerably simplify the implementation of this requirement, because of the security guarantees that such a certification can bring.	

DEV-02 SECURE DEVELOPMENT ENVIRONMENT

Objective

The development environment takes information security in consideration.

Requirements

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

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

DEV-04 SEPARATION OF ENVIRONMENTS

Objective

The development environment takes information security in consideration.

Requirements

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

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

DEV-05 DEVELOPMENT OF SECURITY FEATURES

Objective

The development environment takes information security in consideration.

Requirements

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

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

DEV-06 IDENTIFICATION OF VULNERABILITIES OF THE CLOUD SERVICE

Objective

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

Requirements

Ref	Description	Ass. Level
DEV-06.1	The CSP shall apply appropriate measures to check the cloud service for vulnerabilities that may have been integrated into the cloud service during the development process.	Basic
DEV-06.2	The procedures for identifying vulnerabilities shall be integrated in the development process.	Basic
DEV-06.3	The procedures shall include the following activities, depending on the risk assessment: <ul style="list-style-type: none"> • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. 	Substantial
DEV-06.4	Code reviews shall be regularly performed by qualified personnel or contractors	High
DEV-06.5	The CSP shall assess the severity of identified vulnerabilities according to the criteria defined in OPS-17 and measures are taken to immediately eliminate or mitigate them.	Substantial
DEV-06.6	The procedures for identifying such vulnerabilities also shall include annual code reviews and security penetration tests by subject matter experts, as part of the annual programme defined in OPS-19	High

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

DEV-07 OUTSOURCING OF THE DEVELOPMENT

Objective

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

Requirements

Ref	Description	Ass. Level
DEV-07.1	<p>When outsourcing development of the cloud service or components thereof to a contractor, the CSP and the contractor shall contractually agree on specifications regarding at least the following aspects:</p> <ul style="list-style-type: none"> • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; • Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities. 	Basic
DEV-07.2	<p>Before subcontracting the development of the cloud service or components thereof, the CSP shall conduct a risk assessment according to RM-01 that considers at least the following aspects</p> <ul style="list-style-type: none"> • Management of source code by the subcontractor; • Human resource procedures implemented by the subcontractor; and • Required access to the CSP's development, testing and pre-production environments. 	Substantial
DEV-07.3	<p>The CSP shall document and implement a procedure that makes it possible to supervise and control the outsourced development activity, in order to ensure that the outsourced development activity is compliant with the secure development policy of the service provider and makes it possible to achieve a level of security of the external development that is equivalent to that of internal development</p>	High
DEV-07.4	<p>Internal or external employees of the CSP shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.</p>	High

A.14 PROCUREMENT MANAGEMENT

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

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

Objective

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

Requirements

Ref	Description	Ass. Level
PM-01.1	The CSP shall document, communicate and implement policies and procedures according to ISP-02 for controlling and monitoring third parties whose products or services contribute to the provision of the cloud service:	Basic
PM-01.2	The policies and procedures defined in PM-01.1 shall cover at least the following aspects: <ul style="list-style-type: none"> • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the CSP; • Information security requirements for the processing, storage, or transmission of information by third parties based on recognized industry standards; • Information security awareness and training requirements for staff; • Applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents, and malfunctions; • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers, also contribute to the provision of the cloud service. 	Substantial
PM-01.3	The CSP shall contractually require its subservice organizations to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system with respect to the EUCS requirements.	High
PM-01.4	The reports shall include the complementary subservice organisation controls that are required, together with the controls of the Cloud Service Provider, to meet the applicable EUCS requirements with reasonable assurance	High
PM-01.5	In case the supplier organizations are not able to provide an EUCS compliance report, the CSP shall reserve the right to audit them to assess the suitability and effectiveness of the service-related internal and complementary controls by qualified personnel	High

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

PM-02 RISK ASSESSMENT OF SUPPLIERS

Objective

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

Requirements

Ref	Description	Ass. Level
PM-02.1	The CSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of third parties before they start contributing to the provision of the cloud service:	Basic
PM-02.2	The risk assessment shall include the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects: <ul style="list-style-type: none"> • Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; • The CSP's dependence on the service provider or supplier for the scope, complexity, and uniqueness of the purchased service, including the consideration of possible alternatives. 	Substantial
PM-02.3	Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of Complementary Subservice Organization Controls (CSOC) to be implemented by the subservice provider	Basic
PM-02.4	The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available evidence supporting the assessment of their effectiveness to the targeted evaluation level	Basic
PM-02.5	The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually	Basic

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

PM-03 DIRECTORY OF SUPPLIERS

Objective

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

Requirements

Ref	Description	Ass. Level
PM-03.1	The CSP shall maintain a directory for controlling and monitoring the suppliers who contribute to the delivery of the cloud service	Basic
PM-03.2	The directory shall contain the following information: <ul style="list-style-type: none"> • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the service provider/supplier; • Responsible contact person at the cloud service provider; 	Substantial

Ref	Description	Ass. Level
	<ul style="list-style-type: none"> • Description of the service; • Classification based on the risk assessment; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements. 	
PM-03.3	The CSP shall verify the directory for completeness, accuracy and validity at least annually	Basic

PM-04 MONITORING OF COMPLIANCE WITH REQUIREMENTS

Objective

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

Requirements

Ref	Description	Ass. Level
PM-04.1	The CSP shall monitor the compliance of its suppliers with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of third-parties	Basic
PM-04.2	Monitoring activities shall include at least a regular review of the following evidence, as provided by suppliers under contractual agreements: <ul style="list-style-type: none"> • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards; • independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents, and malfunctions. 	Substantial
PM-04.3	The frequency of the monitoring shall correspond to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. PM-02), and the results of the monitoring shall be included in the review of the third party's risk assessment.	Basic
PM-04.4	Identified violations and deviations shall be analysed, evaluated and treated in accordance with the risk management procedure (cf. RM-01)	Basic
PM-04.5	When a change in a third-party contributing to the delivery of the cloud service affects its level of security, the CSP shall inform all of its CSCs without delay	Basic
PM-04.6	The CSP shall document and implement a procedure to review and update, at least once a year, non-disclosure or confidentiality requirements regarding suppliers contributing to the delivery of the service	Substantial
PM-04.7	The CSP shall supplement procedures for monitoring compliance with automatic monitoring, by leveraging automatic procedures relating to the following aspects: <ul style="list-style-type: none"> • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling). 	High
PM-04.8	The CSP shall automatically monitor Identified violations and discrepancies, and these shall be automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action	High

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

PM-05 EXIT STRATEGY

Objective

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

Requirements

Ref	Description	Ass. Level
PM-05.1	The CSP shall define exit strategies for the purchase of services where the risk assessment of the suppliers identified a very high dependency	Basic
PM-05.2	<p>The exit strategies shall be aligned with operational continuity plans and include the following aspects:</p> <ul style="list-style-type: none"> • Analysis of the potential costs, impacts, resources, and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities, and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; • Definition of indicators for service performance monitoring, which should initiate the withdrawal from the service if the results are unacceptable. 	Substantial

A.15 INCIDENT MANAGEMENT

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

IM-01 POLICY FOR SECURITY INCIDENT MANAGEMENT

Objective

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

Requirements

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

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

IM-02 PROCESSING OF SECURITY INCIDENTS

Objective

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

Requirements

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

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

IM-03 DOCUMENTATION AND REPORTING OF SECURITY INCIDENTS

Objective

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

Requirements

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

IM-04 USER’S DUTY TO REPORT SECURITY INCIDENTS

Objective

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

Requirements

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

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

Objective

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

Requirements

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

IM-06 EVALUATION AND LEARNING PROCESS

Objective

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

Requirements

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

IM-07 INCIDENT EVIDENCE PRESERVATION

Objective

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

Requirements

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

A.16 BUSINESS CONTINUITY

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

BC-01 BUSINESS CONTINUITY POLICIES AND TOP MANAGEMENT RESPONSIBILITY

Objective

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

Requirements

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

BC-02 BUSINESS IMPACT ANALYSIS PROCEDURES

Objective

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

Requirements

Ref	Description	Ass. Level
BC-02.1	The policies and procedures for business continuity and contingency management shall include the need to perform a business impact analysis to determine the impact of any malfunction to the cloud service or enterprise.	Basic
BC-02.2	The business impact analysis policies and procedures shall consider at least the following aspects: <ul style="list-style-type: none"> • Possible scenarios based on a risk analysis; • Identification of critical products and services; • Identification of dependencies, including processes (including resources required), applications, business partners and third parties; • Identification of threats to critical products and services; • Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and • Estimation of the resources needed for resumption. 	Substantial
BC-02.3	The business impact analysis resulting from these policies and procedures shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Substantial

BC-03 BUSINESS CONTINUITY AND CONTINGENCY PLANNING

Objective

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

Requirements

Ref	Description	Ass. Level
BC-03.1	The CSP shall document and implement a business continuity plan and contingency plans to ensure continuity of the services, taking into account information security constraints and the results of the business impact analysis	Basic
BC-03.2	The business continuity plan and contingency plans shall be based on industry-accepted standards and shall document which standards are being used	Substantial
BC-03.3	The business continuity plan and contingency plans shall cover at least the following aspects: <ul style="list-style-type: none"> • Defined purpose and scope, including relevant business processes and dependencies; • Accessibility and comprehensibility of the plans for persons who are to act accordingly; • Ownership by at least one designated person responsible for review, updating and approval; • Defined communication channels, roles and responsibilities including notification of the customer; • Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers); • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management. 	Substantial
BC-03.4	The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Substantial

BC-04 BUSINESS CONTINUITY TESTS AND EXERCISES

Objective

The business continuity framework is tested on a regular basis.

Requirements

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

A.17 COMPLIANCE

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

CO-01 IDENTIFICATION OF APPLICABLE COMPLIANCE REQUIREMENTS

Objective

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

Requirements

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

Guidance elements

CO-01.1	<p>Typically, such requirements may include:</p> <ul style="list-style-type: none"> • Requirements for the protection of personal data (e.g. EU General Data Protection Regulation); • Compliance requirements based on contractual obligations with cloud customers (e.g. ISO/IEC 27001, SOC 2, PCI-DSS); • Generally accepted accounting principles (e.g. in accordance with HGB or IFRS); • National laws
---------	--

CO-02 POLICY FOR PLANNING AND CONDUCTING AUDITS

Objective

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

Requirements

Ref	Description	Ass. Level
CO-02.1	<p>The CSP shall document, communicate, make available and implement policies and procedures for planning and conducting audits, made in accordance with ISP-02 and addressing at least the following aspects:</p> <ul style="list-style-type: none"> • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities. 	Basic

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

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

CO-03 INTERNAL AUDITS OF THE INTERNAL CONTROL SYSTEM

Objective

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

Requirements

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

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

CO-04 INFORMATION ON INTERNAL CONTROL SYSTEM ASSESSMENT

Objective

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

Requirements

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

A.18 USER DOCUMENTATION

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

DOC-01 GUIDELINES AND RECOMMENDATIONS FOR CLOUD CUSTOMERS

Objective

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

Requirements

Ref	Description	Ass. Level
DOC-01.1	The CSP shall make publicly available guidelines and recommendations to assist CSCs with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided	Basic
DOC-01.2	The guidelines and recommendations for the secure use of the cloud service shall cover at least the following aspects, where applicable to the cloud service: <ul style="list-style-type: none"> • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms; • Roles and rights concept including combinations that result in an elevated risk; • Services and functions for administration of the cloud service by privileged users, and • Complementary Customer Controls (CCCs). 	Substantial
DOC-01.3	The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use	Basic
DOC-01.4	The CSP shall describe in the user documentation all risks shared with the customer	Substantial
DOC-01.5	The CSP shall regularly analyse how the CSCs apply the security recommendations and CCCs, and take measure to encourage compliance based on the defined shared responsibility model	High

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

DOC-02 ONLINE REGISTER OF KNOWN VULNERABILITIES

Objective

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

Requirements

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

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

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

DOC-03 LOCATIONS OF DATA PROCESSING AND STORAGE

Objective

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

Requirements

Ref	Description	Ass. Level
DOC-03.1	The CSP shall provide comprehensible and transparent information on: <ul style="list-style-type: none"> • Its jurisdiction; and • System component locations, including its subcontractors, where the cloud customer's data is processed, stored and backed up. 	Basic
DOC-03.2	The CSP shall provide sufficient information for subject matter experts of the CSC to determine to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective	Basic
DOC-03.3	The CSP shall provide information about <ul style="list-style-type: none"> • The locations from administration and supervision may be carried out on the cloud service; • The locations to which any cloud customer data, meta-data or derived data may be transferred, processed or stored. 	Substantial
DOC-03.4	The CSP shall document the locations from which it conducts support operations for clients, and it shall document the list of operations that can be carried by client support in each location	High

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

DOC-04 JUSTIFICATION OF THE TARGETED ASSURANCE LEVEL

Objective

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

Requirements

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

DOC-05 GUIDELINES AND RECOMMENDATIONS FOR COMPOSITION

Objective

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

Requirements

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

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

DOC-06 CONTRIBUTION TO THE FULFILMENT OF REQUIREMENTS FOR COMPOSITION

Objective

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

Requirements

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

A.19 DEALING WITH INVESTIGATION REQUESTS FROM GOVERNMENT AGENCIES

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

INQ-01 LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRIES

Objective

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

Requirements

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

INQ-02 INFORMING CLOUD CUSTOMERS ABOUT INVESTIGATION REQUESTS

Objective

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

Requirements

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

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

Objective

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

Requirements

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

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

A.20 PRODUCT SAFETY AND SECURITY (PSS)

Provide appropriate mechanisms for cloud customers

Foreword for Reviewers

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

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

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

PSS-01 ERROR HANDLING AND LOGGING MECHANISMS

Objective

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

Requirements

Ref	Description	Ass. Level
PSS-01.1	The CSP shall offer to their CSCs error handling and logging mechanisms that allow them to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides	Basic
PSS-01.2	The information provided shall be detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: <ul style="list-style-type: none"> • Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); • Malfunctions during processing of automatic or manual actions; and • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. 	Substantial
PSS-01.3	The logged information shall be protected from unauthorised access and modification and can be deleted by the CSC	Substantial
PSS-01.4	When the CSC is responsible for the activation or type and scope of logging, the CSP shall provide appropriate logging capabilities	Substantial
PSS-01.5	The CSP shall make the information available to CSCs via documented interfaces that are suitable for further processing this information as part of their Security Information and Event Management (SIEM).	High

PSS-02 SESSION MANAGEMENT

Objective

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

Requirements

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

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

PSS-03 SOFTWARE DEFINED NETWORKING

Objective

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

Requirements

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

PSS-04 IMAGES FOR VIRTUAL MACHINES AND CONTAINERS

Objective

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

Requirements

Ref	Description	Ass. Level
PSS-04.1	The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: <ul style="list-style-type: none"> The CSC can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this CSC can only launch the images or containers released according to these restrictions. In addition, these images provided by the CSP are hardened according to generally accepted industry standards. 	Basic
PSS-04.2	The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service: <ul style="list-style-type: none"> If the CSP provides images of virtual machines or containers to the CSC, the CSP appropriately inform the CSC of the changes made to the previous version. 	Substantial
PSS-04.3	An integrity check shall be performed and automatically monitored to detect image manipulations and reported to the CSC at start-up and runtime of virtual machine or container images	High

PSS-05 LOCATIONS OF DATA PROCESSING AND STORAGE

Objective

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

Requirements

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

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

ANNEX B: META-APPROACH FOR THE ASSESSMENT OF CLOUD SERVICES

PURPOSE	This annex describes a meta-approach that is applicable to all conformity assessment for all assurance levels
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 8, Evaluation Methods and Criteria

Foreword for Reviewers

The content related to assessment has recently been structured, and in particular, the assessment for levels Substantial and High is now split between two annexes. This organization is not necessarily permanent and may be reconsidered.

The current proposal is built on the following hypotheses:

- All CSPs are subject to the same requirements in order to get their cloud services certified, regardless of the way in which their cloud services are implemented (e.g., a SaaS provider implementing a full stack vs. a SaaS provider using a subservice provider's infrastructure for the delivery of its own service).
- The auditor is in charge of assessing the level of compliance and assurance for subservice providers based solely on the information available, including assurance reports of various origins and evidence provided by the CSP in their risk assessment of their subservice providers.

As we added more details, such as requirements for documents, these aspects have been the subject of discussions until the last days before the release of this draft candidate scheme.

B.1 INTRODUCTION

B.1.1 Definitions

Audit

In EUCS, the definition of an audit is taken from [ISO17000]:

- A systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled.

ISAE/ISA proposes another definition for the term:

- A systematic process of objectively obtaining and evaluating evidence regarding management assertions about conformity with the predefined framework to ascertain the degree of correspondence between those assertions and established criteria and [additional to ISO] communicating the results to interested users.

For the purpose of this annex, we will consider that the definitions are sufficiently close to be considered equivalent.

Reasonable assurance

A reasonable assurance engagement²¹ is defined in [ISAE3000] as:

An assurance engagement in which the practitioner²² reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the practitioner's conclusion. The practitioner's conclusion is expressed in a form that conveys the practitioner's opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.

Reasonable assurance aims at reducing to an acceptably low level the risk of reaching an inappropriate conclusion when the information provided on the subject matter (here, the description of the cloud service and the CSP's management claim) is materially misstated. Such risk is never reduced to nil and therefore, there can never be absolute assurance.

The conclusion in a reasonable assurance engagement is framed in a positive sense: "Based on the procedures performed, in our opinion, the cloud service XYZ satisfies the requirements of the EUCS at level LLL."

Limited Assurance

A limited assurance engagement is defined in [ISAE3000] as:

An assurance engagement in which the practitioner reduces engagement risk to a level that is acceptable in the circumstances of the engagement but where that risk is greater than for a reasonable assurance engagement as the basis for expressing a conclusion in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the practitioner's attention to cause the practitioner to believe the subject matter information is materially misstated. The nature, timing, and extent of procedures performed in a limited assurance engagement is limited compared with that necessary in a reasonable assurance engagement but is planned to obtain a level of assurance that is, in the practitioner's professional judgment, meaningful. To be meaningful, the level of assurance obtained by the practitioner is likely to enhance the intended users' confidence about the subject matter information to a degree that is clearly more than inconsequential.

For a limited assurance engagement the auditor collects less evidence than for a reasonable assurance engagement but sufficient for a negative form of expression of the auditor's conclusion. The practitioner achieves this ordinarily by performing different or fewer tests than those required for reasonable assurance or using smaller sample sizes for the tests performed.

²¹ An audit performed in the context of the EUCS scheme is a kind of assurance engagement.

²² Auditor

In contrast with a reasonable assurance conclusion, the conclusion in a limited assurance engagement is accordingly framed in a negative sense: "Based on the procedures performed, nothing came to our attention to indicate that the cloud service XYZ does not satisfy the requirements of the EUCS at level Basic."

Determination activities

In the conformity assessment of a cloud service, the following determination activities are essential.

Inquiry

Inquiry consists of seeking relevant information or representations of knowledgeable persons. Inquiries range from formal written inquiries to interviews and informal oral inquiries.

Observation

Observation consists of looking at a process or procedure being performed by others, for example, the observation of the performance of control activities. Observation provides evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place, and by the fact that the act of being observed may affect how the process or procedure is performed. Observation is an appropriate way to obtain evidence if there is no documentation of the operation of a control, like segregation of duties. Observation is also useful for physical controls.

Inspection

Inspection is defined in [ISO17000] as the "examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements".

In the context of EUCS, inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or on other media, or a physical examination of evidence. Inspection of records and documents provides evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the implementation of the controls over their production. Inspection is often used to determine whether manual controls are being performed. Evidence could include written explanations, check marks, or other indications of follow-up recorded on documentation.

Re-performance of monitoring activities or manual controls

Obtaining documents used in the monitoring activity or manual control activity and independently re-performing of the procedures. Comparing any exception items identified with those identified by the responsible control owner.

Re-performance of programmed processing

Input test data, manually calculated expected results, and compared actual results of processing to expectations.

B.1.2 Mapping requirements to controls

It is common practice in examinations that follow established assurance standards and criteria catalogues, that CSPs map their internal controls (the technical and organisational measures in place to prevent risks or to detect and correct undesired events) to the requirements/criteria of the standard. The information is typically presented in a statement of applicability (e.g. for ISO 27001 in form a table that outlines which of the controls in ISO 27001 Annex A are applicable and references to further documentation about the applicable controls) or a description about the service-related system of internal control (e.g. attestations based on AICPA SOC 2). Mappings are typically presented per requirement/criterion of the assurance standards with multiple internal controls assigned to each requirement/criterion to demonstrate compliance.

In the EUCS scheme, the criteria are outlined in form of Security Objectives and related Security Requirements in Annex A: (Security Objectives and requirements for Cloud Services). They represent the mandatory baseline per assurance level for which the CSP must demonstrate compliance.

CSPs can map their internal controls per applicable Security Control Objective and related Security Requirements. Re-using existing descriptions can limit additional efforts for the CSP and contribute to the fast adoption of the EUCSA. It also allows the CSP to demonstrate compliance with multiple assurance standards and criteria catalogues during a

single examination (“test once, rely often”). However, this requires the mapping to be complete, accurate and valid. Further, the nature, timing and extent of evaluation procedures applied by the CAB must provide the required level of evidence.

B.1.3 Subservice providers

The cloud services offered to a CSC will in most cases rely on several subservices, which may be provided internally at the CSP, externally by a different CSP, or externally by a provider that does not provide cloud services (e.g., a hosting provider).

In order to complete the conformity assessment of a Cloud service by a CSP that uses subservice providers, it is relevant to identify the subservice providers and apply the relevant procedures outlined below.

ASSESSMENT METHODS

The assessment needs to consider all subservices listed in the description of the service, internally or externally provided. Internal subservices are necessarily in the scope of the assessment, but external subservices can be handled using two different methods:

1. Include the sub-service provider in the scope (inclusive method);
2. Exclude the sub-service provider from the scope (carve out method).

Both methods are dealing with the services provided by a subservice organization, whereby the CSP’s description of its service presents the nature of the services provided by a subservice organization. In both cases, internal and external subservices are treated similarly and considered as provided by subservice organizations.

Inclusive method

With the inclusive Method the subservice provider’s controls to meet the applicable Security Objectives and the related Security Requirements are included in the CSP’s description of its system. The subservice providers are part of the scope of the CSP’s conformity assessment.

Carve-out method

With the carve-out method the subservice organization’s relevant control objectives and related controls are excluded (carved-out) from the CSP’s description of its system. The subservice organizations are not part of the scope of the CSP’s conformity assessment. Instead, the CSP’s description presents those controls that are designed and implemented to monitor the operating, and if applicable the functional, effectiveness of the controls at the subservice organisation. The monitoring activities shall meet the Security Objectives and the related Security Requirements for “Procurement Management (Supply Chain Management)” outlined in the scheme.

SUBSERVICES IN EUCS

In the context of the EUCS scheme, subservices assessed using the inclusive method shall simply be considered as part of the scope of the CSP’s conformity assessment. The CSP shall be responsible for ensuring that all required evidence is available about the subservice organization, about the services it provides, and about these services are integrated in its own systems in the provision of the cloud service to be assessed.

Subservices assessed using the carve-out methods shall be considered at all stages of the conformity assessment, and in particular during the dependency analysis (see B.8). During that phase, the auditor shall review the assurance documentation available for the subservice.

In the rest of this annex and in the following annexes, when subservices are mentioned, the intended meaning is “subservices assessed using the carve-out method”, unless specified otherwise.

B.1.4 Complementary controls

Information security of a cloud service can only be assured, when the involved parties are aware of and follow their individual responsibilities. For the designs of its internal controls the CSP assumes that user entities (CSCs) and

subservice organizations operate complementary controls that work in combination with the CSP’s internal controls to achieve certain objectives.

In the EUCS scheme, the CSP shall present the Complementary Customer Controls (CCCs) and the Complementary Subservice Organization Controls (CSOCs) assumed in the design of its internal controls as part of the description of the cloud service.

If the CSP uses a subservice organization, the CSP shall obtain relevant information about the CCCs that the subservice organization assumed in the design of their internal controls. Relevant information can be obtained from the subservice organization, e.g. in form of descriptions of the cloud service in accordance with this scheme or other assurance reports that require this information as well (e.g. ISAE 3402, AICPA SOC 2 or BSI C5). For these CCCs the CSP has to ensure that appropriate internal controls are in place. During a conformity assessment, the CAB has to evaluate whether the controls related to the CCCs are suitably designed, implemented and operating effectively.

B.1.5 Presentation

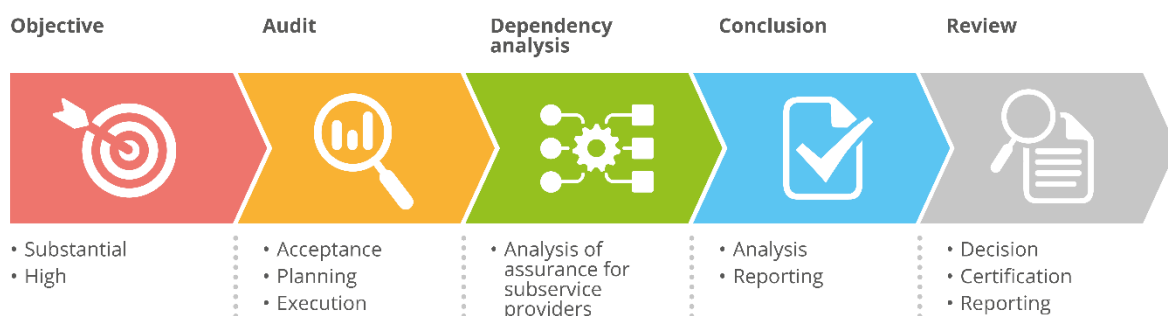
The assessment of cloud services for all levels of the EUCS is based on a meta-approach, which is described here. This meta-approach for assessing and determining conformity describes the overall flow and requirements of the conformity assessment of cloud services in the context of the EUCS scheme.

The meta-approach is the same for all levels, except for the audit itself:

- For the assurance levels Substantial and High, the Conformity Assessment Body (CAB) shall use an audit approach based on either ISO standards or ISAE standards, both complemented with the requirements as defined in this meta approach, leading to providing reasonable assurance, as defined in B.1.1. This approach is described in Annex C: (Assessment for levels Substantial and High).
- For the Basic level, as mentioned in the EU Cybersecurity Act, the CAB shall use a simpler audit approach leading to limited assurance, as defined in B.1.1. This approach is described in Annex D: (Assessment for level Basic).

The structure of this meta-approach starts with defining a clear objective, followed by the development and execution of an audit plan, and ending with the analysis of the gathered evidence and the delivery of an assurance report.

Figure 3: The structure of the Meta-Approach



The term “audit” is used for all conformity assessment activities performed by the audit team and audit team leader (together called “the auditor”) of the CAB, including the analysis of obtained evidence in an assurance report.

To be able to conclude whether all requirements of the EUCS are met, considering the carve-outs and the use of sub service organization, a separate analysis and evaluation needs to take place. This dependency analysis, during which the audit team and audit team leader, or another team designated by the CAB (nevertheless called “the auditor” for simplification), analyses the assurance documentation available for the CSP’s subservice providers, and provides the results in the evaluation report.

The audit report and the evaluation report together may form the basis for awarding a certificate, after review by a team of the CAB independent from the auditor, and together with the delivery of a certification report.

Following [ISO17065], the CAB who issues a certificate is required to perform internally the review and decision activities. However, other activities may be subcontracted, and in particular the audit. Throughout this documentation, the auditor may therefore be part of the CAB or of a subcontractor to the CAB.

B.2 OBJECTIVE OF THE CONFORMITY ASSESSMENT

B.2.1 Introduction

The overall objective of the conformity assessment is to determine whether or not and to what extent a cloud service delivered by a CSP is in conformity with the Security Control Objectives and related Security Requirements defined in the EUCS.

To enable the CAB to perform the conformity assessment the CSP shall prepare and submit an Application Document, including the description of its service that outlines the underlying and supporting processes and the accompanying CSP's statement about the conformity of their cloud service with the requirements of the EUCS. The CSP shall use the template as included in Annex F: (Scheme Document Content requirements) to the EUCS.

The object of the conformity assessment performed by the CAB shall be the cloud service for which a description is provided, and the objective of the conformity assessment is to assess how this cloud service is built and operated with meeting the Security Control Objectives and related Security Requirements as defined in the EUCS. This objective shall be stated in a statement endorsed by the CSP's top management, in a form that complies with the requirements defined in Annex F: (Scheme Document Content requirements).

B.2.2 Basic level

The objective is to provide limited assurance through the execution of an audit (evaluation) by an independent auditor that the cloud service is designed to meet the Security Control Objectives and related Security Requirements as defined in the EUCS that are applicable to assurance level Basic.

The auditor shall obtain sufficient and appropriate evidence by executing audit procedures as defined in Sections D.3 and D.4 about:

- the information presented in the description as provided together with or embedded in the application;
- the suitability of the design of controls to meet the Security Objectives and related Security Requirements; and
- the existence and implementation of these controls as of a specified date during the initial conformity assessment.

B.2.3 Substantial Level

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent auditor that the cloud service is built and operated with procedures and mechanisms to meet the Security Control Objectives and related Security Requirements as defined in the EUCS for the assurance level Substantial.

The auditor shall obtain sufficient and appropriate evidence by executing audit procedures as defined in Sections C.3 and C.4 about:

- the information presented in the description as provided together with or embedded in the application (C.3.1);
- the suitability of the design of controls to meet the Security Control Objectives and related Security Requirements (C.4.1);
- the existence and implementation of these controls as of a specified date during the initial conformity assessment (C.4.2); and
- the operating effectiveness (consistent application) of these controls throughout a specified period in subsequent conformity assessments (C.4.3).

B.2.4 High Level

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent auditor that the cloud service is built and operated with procedures and mechanisms to meet the Security Control Objectives and related Security Requirements as defined by the EUCS for the assurance level High.

The auditor shall obtain sufficient and appropriate evidence by executing audit procedures

As defined in Sections C.3 and C.4 about:

- the information presented in the description as provided together with or embedded in the application (C.3.1);
- the suitability of the design of controls to meet the Security Control Objectives and related Security Requirements (C.4.1);
- the existence and the implementation of these controls as of a specified date during the initial conformity assessment (C.4.2); and
- the operating effectiveness (consistent application) of these controls throughout a specified period in subsequent conformity assessments (C.4.3); and

B.3 ACCEPTING THE CONFORMITY ASSESSMENT ENGAGEMENT

Before agreeing to accept or continue a conformity assessment engagement the CAB shall determine whether the application request is appropriate by performing a review of the application.

The CAB shall conduct a review of the information obtained for application to assess the applicability of the criteria as set in the EUCS, including the decision whether the chosen assurance level is appropriate in the circumstances.

Additional information specific to level Basic are provided in section D.2 and additional information specific to levels Substantial and High are provided in section C.2.

B.4 DEVELOPING THE AUDIT PLAN

The CAB shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the assessment, and determining the nature, timing and extent of planned audit procedures that are required to be carried out in order to achieve the objective of the conformity assessment. This activity shall result in an audit plan, and including aspects that are specific to each assurance level.

In all cases, and for all levels, if the CAB has subcontracted the audit, the CAB may at this point require a review of the audit plan, which shall then be included in the contractual agreement between the CAB and its subcontractor.

Additional information specific to level Basic are provided in section D.3 and additional information specific to levels Substantial and High are provided in section C.3.

B.5 EXECUTION

B.5.1 Introduction

In the phase the auditor shall obtain sufficient and appropriate objective evidence regarding:

- the suitability of the design of controls, including controls over the processes out-sourced to subservice organizations (such as hosting, infrastructure, platform, etc.) to meet the Security Control Objectives and related Security Requirements as defined by the EUCS;
- the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date); and
- for the Substantial and High assurance levels, the operating effectiveness of the implemented controls throughout a period over time (specified period);

Additional information specific to level Basic are provided in section D.4 and additional information specific to levels Substantial and High are provided in section C.4. The auditor shall document the procedures executed, the evidence gained and conclusions reached using the appropriate document (depending on the assurance level).

Figure 4: The structure of the Meta-approach



B.6 ANALYSIS OF RESULTS

Once the auditor has gathered all required evidence, the auditor shall evaluate its sufficiency and appropriateness. This part of the process is specific to every assurance level, with the exception of nonconformity handling, which is common to all three assurance levels and is described below.

Additional information specific to level Basic are provided in section D.5 and additional information specific to levels Substantial and High are provided in section C.5.

B.6.1 Nonconformity handling

If the audit procedures reveal nonconformities (or deviations) in the design, operation or, if required, functionality of the controls, the auditor has to determine whether the applicable Security Requirements of the EUCS were still met. The auditor should consider the following procedures for the determination:

- Notification of the CSP if the nonconformity has been identified by the auditor;
- Inquiry regarding their assessment of the cause of the identified nonconformity;
- Assessment of the CSP’s handling of the identified nonconformity;
- Assessment whether comparable nonconformities have been identified by the CSP’s monitoring processes and what measures have been taken as a result; and
- Qualification of the deviation as minor or major;

These procedures are linked to each other, because the requirements for the handling of an identified nonconformity depend on the qualification of the nonconformity as minor or major. A major nonconformity is defined in [ISO17021] as a “nonconformity that affects the capability of the management system to achieve the intended results”, with a note stating that nonconformities could be qualified as major in the following circumstances:

- there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

In their analysis of nonconformities, CABs should consider both the requirement that is not being fulfilled and the objective to which it refers, to gain an understanding of the impact of the nonconformity to the achievement of the objective.

For a minor nonconformity, the auditor needs to determine that:

- The CSP has determined the cause of the nonconformity;

- The CSP has defined a list of compensating controls that are in place to address the risks arising from the deviation a list of corrective actions to be performed in order to address the nonconformity and a timeline to implement the corrective actions;
- The compensating controls already in place and the corrective actions proposed by the CSP are sufficient to determine that the security requirement is met with the expected level of assurance.

The analysis of compensating controls may include the assessment of alternative organisational and technical measures of the CSP to meet the Security Requirement of the EUCS, which have not been considered in the design of this Security Requirement (e.g. use of new technical measures that provide at least an equal level of security but that are not prescribed in the Security Requirements of the EUCS). Compensating controls are also considered a temporary measure, and nonconformities, even minor, are expected to be corrected in the following conformity assessments. The auditor may therefore define a list of conformity assessment activities to be performed in subsequent conformity assessments.

For a major nonconformity, the auditor needs to determine that:

- The CSP has determined the cause of the nonconformity;
- The CSP has defined and implemented a list of corrective actions to address the nonconformity.
- The corrective actions implemented by the CSP have adequately addressed the nonconformity.

Compensating actions are not allowed for major nonconformities, for which corrective actions shall be defined and implemented in order to obtain or maintain a certificate. Nevertheless, if the corrective actions implemented are sufficient to modify the qualification of the nonconformity as a minor nonconformity, then the remaining nonconformity can be handled as a minor nonconformity, possibly with compensating controls.

The definition of minor and major nonconformities as well as the requirements related to their handling will be refined in guidance provided by ENISA with the support of the ECCG.

Regardless of the qualification of the nonconformities as minor or major, the following information about the CSP's measures to handle such nonconformities and optimise its internal controls shall be disclosed in the assurance report:

- If the nonconformity was detected by the CSP itself, when and in the course of which measures the nonconformity was detected.
- If the nonconformity was already stated in an assurance report of a previous audit, an indication should be given of when and by what means the nonconformity was detected, together with a separate indication that the detection occurred in a previous audit period.
- The measures to be taken to remedy the nonconformity in the future and when these measures are likely to be completed or effectively implemented.

B.7 ISSUING THE ASSURANCE REPORT

After evaluating the result of the audit procedures the auditor shall form a conclusion and issue an assurance report that satisfies the requirements defined in Annex F: (Scheme Document Content requirements) for the targeted assurance level. Additional information specific to level Basic are provided in section D.6 and additional information specific to levels Substantial and High are provided in section C.6

The conclusion shall include the audit team's recommendation as to whether the cloud service satisfies the requirements of the EUCS scheme, pending the results of the dependency analysis. The conclusion shall be based on the evidence obtained and the audit activities performed.

This assurance report shall be first addressed to the CSP. The CSP may contest the content of the assurance report and in particular the audit team's recommendation. If the dispute remains unresolved, the CSP may file a complaint with the NCCA to request their opinion on the matter of the dispute.

B.8 PERFORMING THE DEPENDENCY ANALYSIS

B.8.1 Objectives

The objective of the dependency analysis is to validate that the assurance documentation (assurance reports, certificates) available for the subservices operated by internal or external subservice organisations used by the CSP in the operation of its cloud service are adequate.

For every subservice organisation, the basis for this dependency analysis is the risk assessment of the provider that has been performed by the CSP. As required by EUCS (see Annex A: Security Objectives and requirements for Cloud Services), the assurance report shall contain a rationale explaining how the CSP uses the subservice to satisfy the scheme requirements, and for each subservice a pointer to an assurance component for the subservice.

The dependency analysis consists in analysing these assurance components to determine whether or not the subservice meet the expectations from the CSP at the targeted assurance level.

B.8.2 Assessing the availability of assurance documentation

The first step is to list the assurance documentation available for every subservice provider, and to assess the overall relevance of each assurance component for the dependency review.

The following elements are essential.

About the assurance component itself:

- Type of assurance component, with all required details (e.g., ISO27001 certificate, Type 1 or Type 2 for an ISAE report);
- Period covered or period of validity, possibly complemented with bridge letters or similar statements;
- Applicable framework (existing standard or private framework);
- Inclusion of a mapping to EUCS in the assurance component;

About the auditor's professional competence and independence:

- Name of the CAB or audit organization, name of the audit lead.
- Evidence of the CAB/audit organization's and the auditor's competence (accreditation, personal certification, etc.).
- Evidence of the CAB/audit organization's and the auditor's independence (accreditation, etc.).

By analysing this information, the auditor shall determine whether the assurance documentation available for a given subservice provider is adequate to provide assurance corresponding to the targeted EUCS assurance level.

ENISA, with the support of the ECCG, will issue guidance about the acceptability of different types of assurance components for the different EUCS assurance levels, including potential gaps and attention points.

B.8.3 Assessing assurance related to individual requirements

The second step consists in verifying that the assurance documentation available for the subservice provider is adequate to determine that the subservice provider meets the expectations of the CSP relative to individual EUCS requirements.

This assessment is performed for every subservice provider, and then for every EUCS requirement for which the CSP has declared to rely partially or fully on the assurance provided by the subservice provider, by formulating an assumption on the subservice's control.

The auditor shall for each such assumption determine whether or not the assurance provided in the available assurance documentation is adequate. There are several ways to reach a conclusion that the assurance is adequate:

- The required information is available with the expected assurance level in the assurance documentation.
- The information available in the assurance documentation does not cover the full scope of the requirement, but additional controls implemented by the subservice provider or compensating controls implemented by the CSP allow the auditor to determine that the information is adequate.
- The information available in the assurance documentation does not offer the expected level of assurance, but the controls implemented by the CSP to assess and monitor the subservice provider allow the auditor to determine that the information is adequate.

Finally, if the assurance documentation mentions nonconformities on the controls used to meet an assumption, the corrective measures proposed and implemented by the subservice provider and reviewed by its auditor shall be adequate to guarantee that the assumption is indeed met.

ENISA, with the support of the ECCG, will issue guidance about the adequacy of different types of assurance components for the different EUCS assurance levels, including acceptable additional and compensating controls that may be implemented by the subservice providers and by the CSP.

B.8.4 EUCS-certified subservices

When a subservice has been certified in the EUCS scheme, the processes defined above may be simplified:

- The auditor's competence and independence does not need to be assessed;
- The report can be considered as being fully compliant with the rules of the EUCS scheme for the assurance level of the report;
- No mapping to the EUCS scheme's requirements is needed.

Finally, if the cloud service and its subservice satisfy the requirements for composition, the assessment may be simplified further since the information provided by the subservice organization has already been assessed.

B.9 ISSUING THE EVALUATION REPORT

After evaluating the adequacy of the assurance provided to support assumptions about subservice providers, the auditor shall form a conclusion, combine it with the conclusion from the assurance report, and issue an evaluation report.

The conclusion shall include the audit's team recommendation as to whether the assurance documentation is adequate or not to support the certification of the CSP using these subservice providers. The conclusion shall be based on the audit activities and express whether, in all material respects,

- (i) the audit documentation provided for every subservice provider is adequate to provide assurance corresponding to the targeted EUCS assurance level,
- (ii) for every assumption formulated by the CSP regarding a contribution of a subservice provider to the conformity to an EUCS requirement, the audit documentation provided for that subservice provider is adequate to determine that the assumption formulated by the CSP is correct, with the targeted EUCS assurance level, and
- (iii) for every nonconformity identified in assurance documentation regarding a control used to determine that an assumption formulated by the CSP is correct, appropriate corrective actions have been proposed, implemented and validated by an auditor.

The auditor shall then combine this conclusion of the dependency analysis with the conclusion from the assurance report, for a conclusion regarding the fulfilment of relevant EUCS requirements by the cloud service, and make a recommendation regarding the possible certification of the cloud service under the conditions outlined in the CSP's application.

The auditor shall issue the evaluation report that satisfies the requirements defined in Annex F: (Scheme Document Content requirements).

This dependency report shall be first addressed to the CSP. The CSP may contest the content of the assurance report and in particular the audit team's recommendation. If the dispute remains unresolved, the CSP may file a complaint with the NCCA to request their opinion on the matter of the dispute.

The auditor then delivers the evaluation report, comprising at least the assurance report and the present evaluation report, and if applicable, additional assurance or evaluation reports of sub service providers, to the Conformity Assessment Body (CAB) accredited to issue EUCS certificates, which will then proceed to a review and certification decision.

B.10 REVIEW OF THE EVALUATION

Once an assurance report and an evaluation report (and, if required, supporting reports) have been delivered by the auditor, the CAB shall perform a review of all information and results related to the evaluation, based on these reports:

- The review shall not be subcontracted;
- The review shall be carried out by one or more persons who have not been involved in the audit phase, whom will be called collectively the reviewer;
- The recommendations for a certification decision based on the review shall be documented, unless the review and the certification decision are completed concurrently by the same person;
- The persons carrying out the review shall not normally overturn a negative recommendation of the audit team. If such a situation does arise, the CAB shall document and justify the basis for the decision to overturn the recommendation.

The review shall include at least the following activities:

- A review of the sufficiency of the information provided in the assurance report and supporting documentation with respect to the EUCS requirements and the certification scope;
- A review of the nonconformities identified in the assurance report and related corrective actions
- A review of the issues identified in the evaluation report's dependency analysis; and
- A recommendation for the certification decision, based on a documented opinion on whether or not the requirements of the EUCS have been satisfied by the CSP and by the auditor.

B.10.1 Review of the sufficiency of the assurance report

The CAB shall review the assurance report and supporting documentation concerning the following aspects:

General

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- Does the report contain the required parts?
- Does the provided documentation include the required support documentation?
- Is the conformity assessment performed in due time?

Security controls and requirements

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- If there is a mapping from a set of controls provided by the CSP to the security controls and requirements defined in EUCS, is this mapping adequate?
- For every control or requirement analysed during the audit, have the appropriate activities been performed and documented?

Nonconformities

The CAB shall review the assurance report and supporting documentation concerning the handling of nonconformities detected during the audit.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer.

- For every major nonconformity identified during the audit, is adequate information provided in the assurance report?
- For every minor nonconformity identified during the audit, is adequate information provided in the assurance report?
- For every nonconformity identified during the audit, does the reviewer accept the analysis provided by the auditor?

B.10.2 Review of the evaluation report

Dependency analysis

The CAB shall review the dependency analysis and supporting documentation concerning the adequacy of the assurance documentation available about subservice providers.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- For every subservice provider mentioned in the assurance report, is there adequate assurance documentation available?
- For every assumption in the assurance report about a subservice provider, is the documentation available adequate to determine that assumption correct?

Recommendation for the certification decision

The CAB shall review the recommendation for the certification decision provided in the evaluation report and how it combined the conclusions of the audit report with those of the dependency analysis.

The review shall answer the following questions, with proper justifications. In case of a negative answer, the review shall provide an analysis of the consequences of the negative answer:

- Is the certification decision proposed in the assurance report adequate according to the provided documentation?
- In the case of a maintenance conformity assessment, does the proposed certification decision include all the information required to maintain the certificate, with proper justification?
- If the cloud service depends on subservice providers, is the assurance documentation adequate or not to support the certification of the CSP using these subservice providers?

B.10.3 Review reporting

The results of the review shall be documented in a report, which shall include all the answers to the question above, together with a justification.

If the conformity assessment results in the issuance or maintenance of a certificate, this review report shall be included in the publicly available certification or maintenance report.

B.11 CERTIFICATION DECISION

The CAB shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information. The certification decision shall be carried out by a person or group of persons that has not been involved in the audit activities (but may have been involved in the review process).

The certification decision shall not be subcontracted.

The CAB shall notify the CSP of a decision not to grant certification, to withdraw a certificate, or to suspend a certificate, and shall identify the reasons for the decision. The CSP may contest the CAB's decision. If the dispute remains unresolved, the CSP may file a complaint with the NCCA to request their opinion on the matter of the dispute.

B.12 CERTIFICATION

If the certification decision is negative, i.e. if the cloud service has been determined not to meet the EUCS scheme's requirements, the consequences are as follows:

- In the case of an initial conformity assessment, no further action is required, i.e. no certificate shall be issued;
- In the case of a maintenance conformity assessment, the certificate shall be suspended by appending the maintenance report as rationale for the suspension, and then the process for handling nonconformities shall be followed.

If the certification decision is positive, i.e. if the cloud service has been determined to meet the EUCS scheme's requirements, the consequences are as follows, depending of the nature of the assessment.

- In the case of an initial assessment, the CAB shall issue a new certificate, including the full certification report, and set the expiration date three (3) years after the date of issuance, unless the CAB has explicitly indicated a shorter validity period for the certificate;
- In the case of a periodic assessment, the CAB shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed;
- In the case of a renewal assessment, the CAB shall update the existing certificate by appending the maintenance report, by setting the expiration date of the certificate three (3) years after the date of this update, and if needed by updating elements in the certificate that have changed;
- In the case of a restoration assessment, the CAB shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed, and shall return the certificate's status to "certified";
- In the case of a restoration assessment, the CAB shall update the existing certificate by appending the maintenance report, and if needed by updating elements in the certificate that have changed;

The reports mentioned in the paragraph above are specified in Annex F: (Scheme Document Content requirements).

ANNEX C: ASSESSMENT FOR LEVELS SUBSTANTIAL AND HIGH

PURPOSE	This annex describes the applicable conformity assessment methods for levels 'substantial' and 'high'.
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 8, Evaluation Methods and Criteria

Foreword for Reviewers

This annex has been recently separated from the main meta-approach, in order to support the integration of the conformity assessment method for level Basic with the meta-approach, so there may be a few remaining inconsistencies in the text.

The current proposal is built on the following hypotheses:

- All CSPs are subject to the same requirements in order to get their cloud services certified, regardless of the way in which their cloud services are implemented (e.g., a SaaS provider implementing a full stack vs. a SaaS provider relying on a subservice provider's infrastructure).
- The auditor is in charge of assessing the level of compliance and assurance for subservice providers based on the information available, including assurance reports of various origins and evidence provided by the CSP in their risk assessment of their subservice providers.

Some important templates, described in annexes, are missing, as we first need to determine to which extent they are to be considered as requirements or as guidance.

C.1 INTRODUCTION

The content of this Annex complements the Annex B: (Meta-approach for the assessment of cloud services) for conformity assessments where the CSP claims compliance to the Substantial and High assurance levels.

This Annex follows the content of the Annex B: (Meta-approach for the assessment of cloud services), and refines the definition of the steps related to the audit by providing additional detail.

C.2 ACCEPTING THE CONFORMITY ASSESSMENT ENGAGEMENT

Before agreeing to accept or continue a conformity assessment engagement the CAB shall determine whether the application request is appropriate by performing a review of the application.

The CAB shall conduct a review of the information obtained for application to assess the applicability of the criteria as set in the EUCS scheme, and to ensure that:

- the application request contains all the mandatory information;
- the information about the CSP and the service is sufficient for conducting of the assessment and the certification process, and it fulfils the requirements defined in the EUCS scheme;
- the CSP has acknowledged and understands its responsibilities as set out in Annex F: (Scheme Document Content requirements)
- any known difference in understanding between the CAB and the CSP is resolved, including agreement regarding standards or other normative documents;
- the scope of certification is clearly defined;
- the resources, capabilities and competences are available to perform the conformity assessment activities, including knowledge of the relevant industry, an understanding of information technology and systems and experience in evaluating risks as they relate to the suitable design of controls, and experience in the design and execution of tests of controls and the evaluation of the results.

The CAB may also express its opinion on the suitability of the assurance level selected by the CSP.

In the case of a recertification, the CAB shall also ensure that:

- the reason for the recertification is clearly described; and
- where applicable, the CSP has provided an impact assessment of the changes implemented since the last assessment.

Once all the review criteria are fulfilled and the CAB and CSP have reached an agreement about the conditions of the engagement, the auditor shall conduct the following major audit activities:

1. Developing the audit plan (section C.3);
2. Execution of assessment procedures (section C.4);
3. Analysis of results (section C.5);
4. Issue of an assurance report (section C.6) and of an evaluation report (section B.9).

Once the auditor has delivered the assurance report, the CAB shall perform the following activities:

5. Review of the evaluation (section B.10);
6. Certification decision (section B.11); and
7. Certification (section B.12).

C.3 DEVELOPING THE AUDIT PLAN

C.3.1 Introduction

The CAB shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the assessment, and determining the nature, timing and extent of planned audit procedures that are required to be carried out in order to achieve the objective of the conformity assessment. This activity shall result in an audit plan as described in ISO 19011 and 17021, and including the aspects presented in section C.3.2 and C.3.3 below.

For each activity mentioned below: the auditor shall document the procedures executed, the information and documentation used, the evidence gained, and the conclusion reached, as described in section C.3.3..

C.3.2 Initial activities

In this phase the auditor shall:

- Obtain an Understanding of the CSP's cloud service offered and the controls to meet the Security Control Objectives and related Security Requirements, by reading provided documentation and inquiries of people involved.
 - The auditor shall obtain and read the CSP's description of its system, identify the boundaries of that system, and how it interfaces with other systems (e.g. cloud services provided by subservice organizations) and shall evaluate whether those aspects of the description are fairly presented.
- Assess, if applicable, the mapping between the Security Objectives and related Security Requirements as defined by the EUCS and the CSP's control framework:
 - To conclude whether the applicable Security Objectives and related Security Requirements of the EUCS are covered by the CSP's internal controls;
 - To identify any remaining risks (as a result of gaps in the mapping) and the possible impact of them;
- Determine to what extent and for which elements of the CSP's internal controls sub service organisations are being used and how the CSP controls and monitors the services provided by these sub service organisations;
 - To determine which assessment approach is appropriate: using the inclusive or carve-out method, or a suitable alternative.
 - To identify which sub service organisations do have an acceptable assurance report which can be (re)used.
- Assess how the CSP dealt with complementary controls towards customers of the CSP (user entities) and towards sub service organisations, as well complementary controls of sub service organisations towards the CSP.
- Consider materiality, i.e. the relative importance and effect of possible omissions or deviations with respect to the fair presentation of the description, the suitability of the design of controls and the operating effectiveness of controls, primarily based on qualitative factors, for example: whether the description includes the significant aspects of the cloud systems in accordance with the requirements as defined by the EUCS; whether the description omits or distorts relevant information;
 - Determine to what extent, if any, to use the work of an internal audit function from the CSP and/or to use specific experts;
 - The use of an internal audit function is highly dependent of a number of criteria
 - The use of a specific expert is dependent of the nature of the audit procedure and the complexity of the item to be examined.
- Determine audit procedures to obtain sufficient and appropriate objective evidence about the design, implementation and the operating effectiveness of the CSP's internal controls to meet the Security Control Objectives and related Security Requirements as defined by the EUCS. These procedures are described in the detailed audit plan (C.3.3).
- Determine the roles and responsibilities of the audit team members, as well as guides and observers or interpreters;
- Determine the logistics and communications arrangements, including specific arrangements for the locations to be audited (e.g. datacentre visits);
- Determine matters related to confidentiality and information security of records obtained during the audit;
- Determine any follow-up actions from a previous audit or other source(s) e.g. lessons learned, project reviews.

In the case of a recertification, the auditor shall also:

- Analyse the impact assessment to determine the subset of audit activities that need to be performed in order to cover the changes in the Cloud service since the last assessment; and
- Analyse the reason for the recertification to determine the subset of audit activities that need to be performed in order to satisfy the specific requirements for that trigger (see Annex G:, Certification Lifecycle and continued assurance).

C.3.3 Detailed audit plan

Sufficient and appropriate objective evidence about the design, existence, and operating effectiveness of the CSP's controls shall be gathered using one or more of the following activities: inquiry, observation, inspection, and re-performance of the control and re-performance of programmed processing, as defined in B.1.1.

Detailed reference audit procedures per Security Objectives and related Security Requirements as defined by the EUCS shall be developed, using general guidelines on how to perform some of the audit activities. These references audit procedures shall be the basis for the establishment of the audit plan, but they may need to be adapted to the specific circumstances of the assessment, as explained below.

The CSP's actual approach to meet the Security Objectives and related Security Requirements as defined by the EUCS will be different per CSP. Although they will all have certain elements in common, the actual design, implementation and operation of the controls to meet the security requirements, will be different per organization.

As the actual design, implementation and operation of these controls will be different per organizations, the risks that prevent the CSP from meeting the Security Objectives and related Security Requirements as defined by the EUCS will be different as well. The risks depend e.g. on

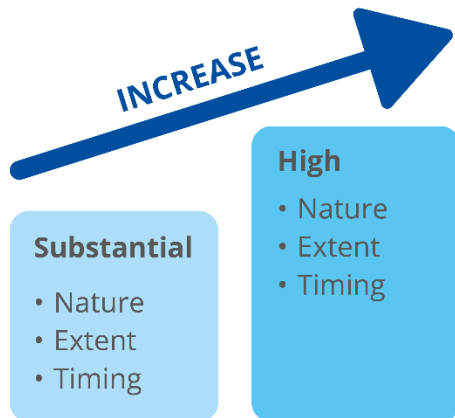
- services provided by the CSP;
- components of the systems used to provide the services;
- environment in which the systems operate.

To deal with this situation, the auditor must be able to tailor the audit procedures for the specific circumstances. By doing so, the following aspects are typically to be considered:

- Whether there have been changes to the systems used to operate the service or the organization (e.g. changes in processes, IT systems);
- The competence of the personnel who perform the measures or monitor its performance and whether there have been changes in key personnel;
- History of errors in the operation of the measures (known from previous examinations);
- The relevance and reliability of the evidence to be obtained;
- The nature of the measures (including their level of automation) and the frequency with which it operates;
- The degree to which the measures rely on the effectiveness of other measures.

The audit procedures need to be adapted to a specific security requirement and desired level of certification. Security requirements have been constructed in a way that all security requirements for level basic are applicable to levels substantial and high, while security requirements for level substantial also apply to level high. Therefore, it is necessary to access all security requirements on the specific level, including those from lower levels. Security requirements that were initially written for level Basic, are also applicable to levels Substantial and High, but they would be assessed in different ways according the certification level.

Figure 5: the Audit procedure



Based on the analysis above the auditor shall determine for each control and security measure under audit:

- the nature (what kind of audit procedure),
- the extent (how many or how often to execute the procedure), and
- the timing (at what point in time or over what period)

of the evidence gathering audit procedures.

NATURE

The nature of an audit procedures relates to the kind of an audit procedures and describes the way how to obtain the evidence required.

Selecting the nature depends on the specific characteristics of the specific control or security measure under audit. The rigour and depth increase from substantial to high assurance level. The different natures of activities are described in section B.1.1.

EXTENT

The extent of an audit procedure relates to the number of observations to be performed, the rigour and dept of inquiries, how many inspections are needed, and the number of re-performances of a specific audit procedure.

Determining the extent depends on the specific characteristics of the control or security measure and the assurance level required. The extent in case of the assurance level high is much higher than for assurance level substantial. In many cases, especially for testing operating effectiveness, a sampling approach is appropriate.

Sampling

The size of the samples to select in order to test the operating effectiveness of controls primarily depends on the nature and frequency of the control. The following sample sizes should provide reasonable assurance that the tested controls operated effectively during the specified period and that the associated control objectives were achieved during that specified period. Where the population of occurrences falls between the levels identified in the table below, the number of items to test shall be interpolated, exercising professional judgment in determining the appropriate sample size.

Table 5: Determining sample size

Frequency of the control	Assumed population of control occurrences	Sample Size (per specified period)
More than daily	Over 250	25 - 60
Daily	250	20 - 40
Weekly	52	5 - 15
Monthly	12	2 - 5
Quarterly	4	2
Annually	1	1

Timing

The timing of an audit procedure relates to the point in time of a period to be covered of an audit procedure.

For obtaining evidence about design and implementation/existence the audit procedures are built around a certain point in time: the reporting date.

For obtaining evidence about operating effectiveness the audit procedure need to cover a period before the reporting date (typically 12 months, or 3-6 months for an initial audit), which is fixed in the scheme and in Annex G: (Certification Lifecycle and continued assurance), depending on the assessment type.

Documentation

The detailed plan shall be documented following the requirements defined in Annex F: (Scheme Document Content requirements) for the “Audit Plan and Execution”.

For each control or security measure under audit the template shall be used covering the following topics:

- the control or security measure under audit;
- for the suitability of the design, the existence and implementation, and operating effectiveness:
 - nature of the audit procedure;
 - timing of the audit procedure;
 - extent of the audit procedure;
- the documents used, the names and function of the inquired people, other information;
- the evidence obtained;
- the conclusion reached.

These procedures will vary between engagements and depends, among other things, on the requested assurance level (Substantial or High) and the auditor’s judgment, including the assessment of the risks of material non-conformity of the matter being investigated. All the three elements increase in scope, depth and rigour as the level of assurance increases.

C.3.4 Audit plan review

The auditor may request the reviewer (see B.10) to provide an opinion on the audit plan, to ensure that they agree on the structure and content of the plan before its execution. The CSP may explicitly request this review to be performed before starting the execution of the audit plan.

C.4 EXECUTION

C.4.1 Suitability of the Design of Controls

A control is suitably designed, when actions or events that comprise a risk (e.g. for information security) are prevented, or detected and corrected. Obtaining evidence regarding the suitability of the design of controls requires the auditor to determine whether

- The risks that threaten the achievement of the Security Control Objectives and related Security Requirements as defined by the EUCS have been identified by the CSP;
- The controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the Security Control Objectives and related Security Requirements of the EUCS from being met.

To be able to conclude on this the auditor shall:

- obtain an understanding of the CSP's process for identifying and evaluating the risks that threaten the achievement of the Security Control Objectives and related Security Requirements and assessing the completeness and accuracy of the CSP's identification of those risks,
- evaluate the linkage of the controls with those risks, which is typically a consideration of frequency or timing of the occurrence or performance of the control (e.g. monthly, weekly, per triggering action or event such as a service request);
- evaluate the party responsible for conducting the control (e.g. competence and authority of the person, group or system);
- understand the specific activity being performed by the party to determine especially how the control is triggered, how it is executed, which tools or systems are used to support the execution and which records are kept evidencing the execution; and
- validate the source of information (for example a log file, archive, ticketing system, etc.) to which the control is applied to determine whether this source is reliable and ensures for completeness and accuracy of information processing.

Obtaining evidence regarding the suitability of the design of controls typically requires the auditor to perform inquiries with the CSP's subject matter experts and the examination of supporting documentation that describe how the control should operate, e.g. written policies, procedures or process flowcharts.

C.4.2 Existence and Implementation of controls and security measures

In order to prevent, or detect and correct actions that comprise a risk, the controls have to be placed in operation as designed.

After the auditor has concluded that a control is suitably designed, it has to be concluded per control whether the control actually exists and is implemented as designed.

To be able to conclude on this the auditor shall obtain evidence that the controls and security measures have been implemented by examining exemplary actions or events that triggered the occurrence or performance of the controls (e.g. tickets) and to inspect the environment in which it operates (e.g. suitable configuration of the tools or systems used to execute the control in accordance with the design).

C.4.3 Operating effectiveness

Controls considered to be suitable in design, shall be tested for operating effectiveness over a certain period of time (specified period). The auditor shall design the tests in a manner to cover a representative number of actions and events that triggered the occurrence or performance of the controls throughout the specified period.

For initial certification the period shall be at least 3 months for level Substantial and 6 months for level High; for subsequent certification the period is 12 months or the time since the operating effectiveness was last tested in a

previous conformity assessment. In all cases, the period to consider shall be the period that precedes immediately the conformity assessment.

In determining the nature, timing and extent of the tests the following the auditor shall consider:

- the nature and frequency of the controls being tested,
- the types of available evidential matter,
- the nature of the Security Control Objectives and related Security Requirements to be met;
- the assessed level of control risk,
- the expected efficiency and effectiveness of the tests, and
- the results of tests of the control environment.

A control is operating effectively, if

- it was consistently applied as designed throughout the specified period, and
- in case of manual controls, they were applied by individuals who have the appropriate competence and authority (e.g. changes being only approved by personnel who are responsible for the service being provided).

To be able to conclude on this the auditor shall perform procedures such as inspection, observation, or re-performance *in combination* with inquiry to obtain evidence about the following:

- how the control was applied;
- the consistency with which the control was applied; and
- by whom or by what means the control was applied.

An inquiry alone is NOT sufficient to determine whether a control operated effectively. This also applies to controls, if applicable, over the out-sourced processes to sub-service providers.

At level High, in addition to the testing for operating effectiveness, the CAB and the CSP shall define procedures for the automated monitoring of key security controls, including at least:

- A description of automated monitoring mechanisms implemented by the CSP;
- A description of the procedures implemented by the CSP to handle the deviations and nonconformities identified through automated monitoring;
- A description of the procedures used to notify the CAB, at least when any major nonconformity is identified through automated evidence gathering.

Specific controls and requirements are defined in Annex A., Security Objectives and requirements for Cloud Services that define the general requirements for these procedures, and also define the minimum set of automated evidence gathering mechanisms to be implemented by the CSP.

C.5 ANALYSIS OF RESULTS

C.5.1 Evaluation of evidence obtained

The auditor shall evaluate the sufficiency and appropriateness of the evidence obtained from the executed audit procedures to conclude about the suitability of the design, existence and implementation, and operating effectiveness.

The evidence obtained shall be appropriate and sufficient to enable the auditor to take informed decisions.

In addition, when using information produced (or provided) by the CSP, the auditor shall evaluate whether this information is reliable enough for executing the planned audit procedures by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was appropriately precise, detailed, consistent and current.

Sufficiency is the measure of the quantity of evidence. The quantity of evidence needed is affected by the risks of that the description is not fairly presented and that the controls were not suitably designed or operating and, if required, functioning effectively, and also by the quality of such evidence (the higher the quality, the less may be required). Obtaining more evidence, however, may not compensate for its poor quality.

Appropriateness is the measure of the quality of evidence; that is, its relevance and its reliability in providing support for the auditor’s opinion. The reliability of evidence is influenced by its source and by its nature, and is dependent on the individual circumstances under which it is obtained.

All relevant evidence shall be considered, regardless of whether it appears to corroborate or to contradict the analysis of the description or the controls against the applicable security requirements of the EUCS.

If the auditor is unable to obtain sufficient appropriate evidence to conclude on a given requirement, then the audit shall be considered inconclusive. This should be considered as a nonconformity, and handled as defined in B.6.1.

C.5.2 Analysis of controls to meet the applicable Security Control Objectives and related Security Requirements of the EUCS

The analysis of the suitability of the design, existence and implementation, and operating effectiveness of the CSP’s internal controls, is based on the requirements outlined in section C.4 above.

For analysing whether the CSP’s internal controls meet the Security Control Objectives and related Security Requirements of the EUCS, the auditor has to consider whether the controls fully cover all aspects of the Security Requirements. Several controls may be required in combination per Security Requirement to fully meet each security requirement.

If the CSP already performs audits in accordance with other standards (e.g. ISO 27001 or SOC 2), it is possible that the controls presented in the description may be optimally aligned with the criteria of these standards, but that their descriptions do not fully meet all aspects of the Security Requirement of the EUCS to which they are mapped to.

The auditor’s test procedures and the results thereof shall be documented in the report according to the examples in the table below

Security Control Objectives	<Service-Org>’s Description of Controls	Tests Performed	Test Results
Objective: description			
ID – Security requirement	ID – Title of Control [Control Description]	Test performed by the auditor	Test result by the auditor

In describing the tests of controls in the assurance report, the auditor shall clearly state per control tested, whether the items tested represent all or a selection of the items in the population. The auditor shall further indicate the nature of the tests in sufficient detail to enable the CAB’s review team as the report recipient to review whether the auditor has obtained sufficient and appropriate objective in accordance with the requirements as outlined in section C.4.

If nonconformities (or deviations) have been identified, the auditor shall record them against a specific control, including a description of the objective evidence on which the nonconformity is based, the extent of testing performed that led to identification of the nonconformities (including the sample size where sampling has been used), and the number and nature of the nonconformities noted. The auditor shall report nonconformities even if, on the basis of tests performed, he has concluded that the related Security Requirement of the EUCS were met, and even if the CSP has implemented corrective actions to address the nonconformities and the auditor has determined that the corrective actions effectively address the nonconformities.

C.6 ISSUING THE ASSURANCE REPORT

After evaluating the result of the audit procedures the auditor shall form a conclusion and issue an assurance report.

The conclusion shall include the audit team's recommendation as to whether the cloud service should be certified or not. The conclusion shall be based on the evidence obtained and the audit activities performed, and express whether, in all material respects,

(1) For Substantial Level:

- (i) the CSP's description fairly presents its cloud service, including the controls to meet the Security Control Objectives and related Security Requirements of the EUCS, and is free from material misstatements as of a specified date (in case of an initial conformity assessment) or throughout a specified period (in case of a subsequent conformity assessment);
- (ii) the controls stated in the CSP's description were suitably designed, existed and were implemented to provide reasonable assurance that the Security Control Objectives and related Security Requirements of the EUCS were met as of a specified date (in case of an initial conformity assessment) or throughout a specified period (in case of a subsequent conformity assessment); and
- (iii) the controls stated in the CSP's description operated effectively to provide reasonable assurance that the Security Control Objectives and related Security Requirements of the EUCS were met throughout a specified period; or.

(2) For High Level:

- (iv) (i) and (ii) above noted for Substantial Level; and
- (v) the controls stated in the CSP's description operated and functioned effectively to provide reasonable assurance that the Security Control Objectives and related Security Requirements of the EUCS were met throughout a specified period.

The auditor shall issue the assurance report using the template in Annex F: (Scheme Document Content requirements).

This assurance report shall be first addressed to the CSP.

ANNEX D: ASSESSMENT FOR LEVEL BASIC

PURPOSE	This annex describes the applicable conformity assessment method for level Basic.
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 8, Evaluation Methods and Criteria

Foreword for Reviewers

This annex has been integrated recently.

Some important templates, described in annexes, are missing, as we first need to determine to which extent they are to be considered as requirements or as guidance. Also, for level Basic, some documents are based on checklists, which will be built with numerous references to the scheme's security requirements, as defined in Annex A: (Security Objectives and requirements for Cloud Services).

D.1 INTRODUCTION

At the Basic assurance level, the conformity assessment is greatly simplified, and it relies solely on evidence provided by the CSP, if needed upon explicit request from the CAB. For consistency reasons, we will use the same terminology (audit, auditor, audit team) as for the other assurance levels, also the evaluation performed is not a full-fledged audit of the cloud service to be certified.

For the assurance level Basic the reviewer shall use the approach defined in the present Annex.

This approach is facilitating a controlled environment for providing limited assurance while keeping the associated cost for certification affordable for smaller CSP's, through limited evaluation of the control framework of the CSP by an independent reviewer that the cloud service is built and operated with procedures and mechanisms to meet the corresponding Security Objectives and related Security Requirements defined in the EUCS.

The EU Cybersecurity Act requires for the assurance level Basic that the evaluation must minimise the known basic risks of incidents and cyberattacks, and that a review of technical documentation is required at a minimum.

While the CSP shall be required to conduct the necessary initial verification of compliance with the objectives and controls of this scheme, at the basic level there will be a review of the documentation created or compiled by the CSP as a part of its internal verifications.

D.2 ACCEPTING THE CONFORMITY ASSESSMENT ENGAGEMENT

Before agreeing to accept or continue a conformity assessment engagement the CAB shall determine whether the application request is appropriate by performing a review of the application.

The CAB shall conduct a review of the information obtained for application to assess the applicability of the criteria as set in the EUCS, including the decision whether the chosen assurance level is appropriate in the circumstances, and to ensure that:

- the application request contains all the mandatory information;
- the information about the CSP and the service is sufficient for conducting of the assessment and the certification process;
- the CSP has acknowledged and understands its responsibilities as set out in TBD
- any known difference in understanding between the CAB and the CSP is resolved, including agreement regarding standards or other normative documents;
- the scope of certification is clearly defined;
- the means are available to perform all evaluation activities;
- the resources, capabilities and competences are available to perform the engagement, including knowledge of the relevant industry, an understanding of information technology and systems and experience in evaluating risks as they relate to the suitable design of controls, and experience in the design and execution of tests of controls and the evaluation of the results.

In addition, the auditor shall obtain a legally binding declaration of the CSP that it acknowledges and understands its responsibility and complies at least, with the following:

- the CSP is responsible for the preparation of the description of its system ("Description"), and accompanying CSP's assertion ("Management Statement");
- if the certification applies to ongoing service provision, the certified service continues to fulfil the security requirements;
- the CSP agrees to on-site reviews in case they would be necessary to clarify assertions or to resolve complaints disputes;
- the CSP makes claims regarding certification consistent with the scope of certification;
- the CSP does not use its service certification in such a manner as to bring the certification body into disrepute and does not make any statement regarding its service certification that the certification body may consider misleading or unauthorized;

- upon suspension, withdrawal, or termination of certification, the CSP discontinues its use of all advertising matter that contains any reference thereto and takes any other required measure, and inform their customers;
- in referring to its service certification in communication media such as documents, brochures or advertising, the CSP complies with the requirements of the certification body;
- the CSP complies with any requirements that may be prescribed in the certification scheme relating to the use of marks of conformity, and on information related to the service;
- the CSP keeps a record of all complaints made known to it relating to compliance with security requirements and makes these records available to the certification body when requested, and
 - takes appropriate action with respect to such complaints and any deficiencies found in service that affect compliance with the security requirements;
 - documents the actions taken;
- the CSP informs the certification body, without delay, of changes that may affect its ability to conform with the certification requirements.
- the CSP agrees to fees payable to the CAB for the execution of the conformity assessment communicated beforehand

In the case of a recertification, the CAB shall also ensure that:

- the trigger for the recertification is clearly described; and
- where applicable, the CSP has provided an impact assessment of the changes implemented since the last assessment.

Once all the review criteria are fulfilled and the CAB and CSP have reached an agreement about the conditions of the engagement, the auditor shall conduct the following major audit activities:

1. Developing the audit plan (section D.3);
2. Execution of assessment procedures (section D.4);
3. Analysis of results (section D.5);
4. Issue of an assurance report (section D.6) and of an evaluation report (section B.9).

Once the auditor has delivered the assurance report, the CAB shall perform the following activities:

5. Review of the evaluation (section B.10);
6. Certification decision (section B.11); and
7. Certification (section B.12).

D.3 DEVELOPING THE AUDIT PLAN

D.3.1 Introduction

The CAB shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the audit to be carried out in order to achieve the objective of the conformity assessment. This can be achieved by using a predefined audit plan.

For each activity mentioned below: the auditor shall document the high-level audit plan following the requirements defined in Annex F: (Scheme Document Content requirements), including the procedures executed, the information and documentation used, the evidence gained, and the conclusion reached.

There shall be at least one meeting between the CAB and the CSP during the development of the audit plan, to provide clarifications about the cloud service and related controls and about the next phases of the audit.

D.3.2 Initial activities

In this phase the assessor shall:

- Obtain an Understanding of the CSP's cloud service offered and the controls to meet the Security Control Objectives and related Security Requirements, by reading provided documentation and inquiries of people involved.
 - The auditor shall obtain and read the CSP's description of its system, identify the boundaries of that system, and how it interfaces with other systems (e.g. cloud services provided by subservice organizations) and shall evaluate whether those aspects of the description are fairly presented.
- Review the CSP's mapping between the Security Objectives and related Security Requirements as defined by the EUCS and the CSP's control framework:
 - To conclude whether the applicable Security Control Objectives and related Security Requirements of the EUCS are covered by the CSP's internal controls;
 - To identify any remaining risks (as a result of gaps in the mapping) and the possible impact of them;
- Determine to what extent and for which processes the CSP uses sub service providers and how the CSP controls and monitors the services provided by these sub service providers;
 - To determine which assessment approach is appropriate: using the inclusive or carve-out method.
 - To identify which sub service providers do have an acceptable assurance report which can be (re)used.
- Review how the CSP dealt with complementary controls towards customers of the CSP (user entities) and towards sub service providers, as well complementary controls of sub service providers towards the CSP:
 - Does the CSP has CCC for its costumer defined?
 - Does the CSP fulfils the CCC of the subservice provider for the services consumed?
- Consider the relative importance and effect of possible omissions or deviations with respect to the fair presentation of the description,
 - whether the description includes the significant aspects of the cloud systems;
 - whether the description omits or distorts relevant information;
- Determine self-assessment and audit procedures to obtain sufficient and appropriate objective evidence about the design and implementation of the CSP's internal controls to meet the Security Control Objectives and related Security Requirements as defined by the EUCS by using a review plan.

D.3.3 The audit plan

Sufficient and appropriate objective evidence about the design and implementation of the CSP's internal controls can be obtained through, inspection of the provided documentary evidence and if necessary, by inquiry to be able to evaluate the provided documentary evidence in order to determine whether

1. the evidence addresses the security requirements of the scheme in a sufficiently comprehensive manner;
2. the evidence is sufficiently clear and unambiguous in how the requirements are met and how controls have been implemented by the CSP;
3. the evidence is *prima facie* plausible (i.e. it appears in the professional opinion of the reviewer that there are no elements in the evidence that are manifestly inaccurate, incomplete or false) and verifiable (can in principle be verified by an on-site audit).

This can be achieved by using a standardized self-assessment and audit plan (To be developed), The CAB shall then provide the self-assessment plan to the CSP, together with indications on its specific application to the targeted cloud service.

D.4 EXECUTION

In the phase the auditor shall obtain sufficient and appropriate objective evidence by evaluation the provided documentary evidence by the CSP regarding:

- the suitability of the design of controls, including controls over the out-sourced processes (such as hosting, infrastructure, platform, etc.) to meet the Security Control Objectives and related Security Requirements as defined by the EUCS;
- the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date).

The execution phase starts when the CSP provides the results of their self-assessment, together with all required supporting documentation. The auditor shall document the procedures executed, the evidence gained and conclusions reached using a standardized document (To be developed)

A control is suitably designed when actions or events that comprise a risk (e.g. for information security) are prevented or detected and corrected. Obtaining evidence regarding the suitability of the design of controls requires the auditor to determine whether

- The risks that threaten the achievement of the Security Control Objectives and related Security Requirements as defined by the EUCS have been identified by management;
- The controls are, if operating effectively, able to prevent or detect Security Control Objectives and related Security Requirements of the EUCS from not being met.

In order to prevent, or detect and correct actions that comprise a risk, the controls have to be placed in operation as designed. After the auditor has concluded that a control is suitably designed, it has to be concluded per control whether the control actually exists and is implemented as designed by examining the provided documentary evidence. To be able to conclude on this the reviewer shall obtain evidence related to exemplary actions or events that triggered the occurrence or performance of the controls (e.g. tickets) and to inspect the environment in which it operates (e.g. suitable configuration of the tools or systems used to execute the control in accordance with the design).

D.5 ANALYSIS OF RESULTS

In forming the conclusions on the evidence obtained the auditor shall

1. Evaluate whether the described technical and organizational controls refer to or describe the applicable requirements of the Certification framework;
2. Consider whether the provided documents adequately disclose the significant information security policies and the selected and implemented technical and organizational measures;
3. Consider whether the information security policies and technical and organizational measures are deemed suitable to meet the Security Control Objectives and related Security Requirements of the EUCS considering the nature of the service;
4. The information provided appears relevant, reliable, comprehensive and comparable.

On this basis the auditor shall assess if it can be concluded that nothing has come to its attention that causes the reviewer to believe that the technical and organizational manners warranted by the CSP are not meeting in all material aspects the requirements of the Basic level in accordance with the Certification framework and that the evidence presented is at least sufficient for the reviewer to obtain a limited level of assurance.

The auditor shall document the results of the review in the report according to the examples in the (mapping) table below.

Security Control Objectives	<Service-Org>'s Description of Controls	Documentary evidence used or other means of evidence	Test Results
Objective: description			
ID – Security requirement	ID – Title of Control [Control Description]	Description of the evidence	Result

There shall be at least one meeting between the CAB and the CSP during the execution phase or the analysis of results, during which the CAB may ask for additional documentation or make specific inquiries to consolidate the evidence and the analysis of results.

D.6 ISSUING THE ASSURANCE REPORT

After evaluating the result of the audit procedures, the auditor shall form a conclusion and issue an evaluation report.

The conclusion shall be based on the evidence obtained and the procedures performed, and express whether, in all material respects, nothing has come to the reviewer's attention that the

- i. CSP's description does not fairly presents its cloud service, including the controls to meet the Security Control Objectives and related Security Requirements of the EUCS, and is free from material misstatements as of a specified date;
- ii. controls stated in the CSP's are not in conformity with the Security Control Objectives and related Security Requirements of the EUCS as of a specified date.

The reviewer shall issue the assurance report using the template in Annex F: (Scheme Document Content requirements).

This assurance report shall be first addressed to the CSP.

ANNEX E: COMPETENCE REQUIREMENTS FOR CABS

PURPOSE	This annex describes the competence requirements for CABS for the various levels
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 7, Specific requirements applicable to a CAB

Foreword for Reviewers

The content of this Annex will be developed together with the requirements for accreditation for the scheme, whose development will be initiated after the external review.

ANNEX F: SCHEME DOCUMENT CONTENT REQUIREMENTS

PURPOSE	This annex describes the applicable requirements on the minimum content to be included in the scheme documents
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter

Foreword for Reviewers

The content of this Annex specifies requirements regarding the content of documents to be used in the scheme.

Some of these requirements have been defined very late in the development of the draft candidate scheme, and they have not gone through a full review by the members ad hoc working group.

F.1 INTRODUCTION

The objective of this Annex is to define guidelines for the redaction of documents. Rather than providing full templates, the Annex lists requirements for writing the documents, which typically takes three forms:

- Requirements on content that shall be present, without constraints on the format;
- Requirements on text that shall be included as is, for a few important statements; and
- Requirements on the format and content of tables, to ease comparability of results.

These requirements will be refined by specific guidance for every assessment type (ISO-based, ISAE-based, or EBCA).

F.1.1 Conventions used in this annex

Every section below starts with an introduction, followed by the requirements on the document, presented in a sequential manner that defines the structure of the document.

Within each section, this annex uses with the following convention:

- Requirements are typeset in plain text.
- Guidance is typeset in *italics*.
- Mandatory text is typeset in **bold**.
- Items in a document are referenced by an identifier, which is defined within brackets in <SMALL CAPS>

The rules for using these requirements are as follows:

- Specified sections shall be present, in the order defined, but other sections may be added before, between and after the specified sections;
- Within a section, mandatory text shall be present and the section's requirements shall be fulfilled, but additional content may be added;

F.1.2 List of the documents

Requirements and guidance are provided in this annex for the following documents:

- For the application phase
 - i) The Application Document, to be filled out by the CSP to initiate a conformity assessment
- For the audit preparation phase
 - i) The Initial Activities Planning document, to be prepared by the CSP at the beginning of the conformity assessment
 - ii) The Detailed Audit Plan and Execution, to be prepared by the CSP before the audit and updated with the results all along the audit.
- For the reporting phase
 - i) The Assurance Report, to be prepared by the CAB to report on the audit of the cloud service from the CSP.
 - ii) The Evaluation Report, to be prepared by the CAB to report on the assurance provided by the CSP's subservice providers and to conclude on the audit by providing a certification recommendation.
 - iii) The Review Report, to be prepared by the CAB after the internal review of the Assurance and Evaluation Reports.
- For the certification phase
 - i) The Certification Report, to be prepared by the CAB when the certificate is issued
- For the maintenance phase
 - i) The Impact Analysis Report, to be prepared by the CAB when a request about a potential nonconformity or vulnerability does not lead to a conformity assessment.
 - ii) The Maintenance Report, to be prepared by the CAB after a maintenance conformity assessment, with a focus on the updates to the cloud service and on the reason that triggered the conformity assessment

These documents do not all have the same usage and availability:

- The Application Document, Assurance Report and Evaluation Report are shared between the CSP and the CAB.
- In addition, the CSP shall make the Assurance Report available to its customers upon request.
- The Initial Activities Planning, Detailed Audit Plan and Execution, and the Review Report are internal documents for the CAB.
- The Certification Report is a public document, to be published together with the certificate.

All documents may be made available by the CAB to the NCCA and NAB for review or assessment.

Finally, the Assurance Report is only available in a version suitable for the Substantial and High assurance levels. A version suitable for the Basic assurance level will be provided in a later phase. Requirements for the Review Report, for the Impact Analysis Report and for the Maintenance Report are not available in the current version.

F.2 APPLICATION DOCUMENT

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Application Document”.

A CSP shall apply these requirements in its application for certification of a cloud service. The document shall include the information a CAB needs to start a conformity assessment. The completed template provides evidence of a self-assessment process executed by the management of the CSP.

Mandatory field in the template	Clarification
Section 1: “Identification” This section identifies the Cloud Service for which the evaluation application is submitted.	
CSP Identity	Identity of the CSP requesting the evaluation.
CSP Contact	Identification and contact details for the lead contact at the CSP that will support the evaluation process.
Service Name	Commercial name of the CSP Cloud Service for which the evaluation is requested.
Short Description	A short description of the functionality of ‘Service Name’.
Assurance Level	The assurance level for which the evaluation is requested. Valid values are ‘Basic’, ‘Substantial’, or ‘High’.
Security Profiles	The list of security profiles applicable to the cloud service
Application Type	CSP specified evaluation application type. Valid values are ‘initial’, ‘periodic’, ‘renewal’ or ‘restoration’.
Application Period	When applicable, the period to be considered by the CAB for the assessment of operational effectiveness.
Section 2: “Claim” This section is the CSP’s management assertion the template accurately and fairly describes the Cloud Service and the applicable controls from the scheme’s framework.	
Claim	This is a written conformity statement by the management of the CSP.
Section 3: “CSP’s Description of its service” This section is the CSP’s assessment of the Cloud Service’s implementation of the scheme’s requirements and control framework.	
3.1: Types of Services	The specific functional purposes of the Cloud Service.
3.2: Service Components	This is a document label for reference purpose, no text required.
- Physical Infrastructure	The physical structures of the service, datacentre, server, other hardware.
- Software	The programs and system software that supports programs, that are part of the service
- People	The personnel involved in the governance, operation and use of a service
- Policies and procedures	The policies and automated and manual procedures involved in the operation of a service
- Data	the information used and supported by a service (transaction streams, files, databases and tables).
3.3: Service Boundaries	The boundaries of the system subject to certification
3.4: Sub Services	The sub-services that are material to the operation of the Cloud Service

Mandatory field in the template	Clarification
3.6: Information for customers	Reference to the scheme's control requirements framework
- Supplementary information	List of the supplementary information to be made publicly available by the CSP
- Transparency information	
- Complementary Customer Controls, CCC	List the applicable CCCs
3.7: Other information	Additional information the CSP considers relevant to the evaluation of adherence to the Scheme framework.
<p>Section 4: "CSP's description of its security controls" This section is the CSP's description of the implemented controls, and of their mapping to the EUCS objectives and requirements.</p>	
Control objectives	The security objectives and CSPs description of controls

CONTENT OF THE DOCUMENT

F.2.1 Identification

<CSP IDENTITY>

The CSP identity shall include at least:

- Commercial name of the organization;
- Legal name of the organization;
- Registration number in Chamber of Commerce or equivalent;
- Office and headquarter location; and
- Contact details of the person that is legally representing the organization

When a consortium or joint venture is an applicant, all participating parties with legally representing persons shall be clearly indicated, including all registration details.

<CSP CONTACT>

The CSP Contact shall be the primary contact at the CSP for the CAB. It can be an individual person or a CSP assigned group name. It shall include at least the name of the responsible department and contact details (phone number and email address).

<SERVICE NAME>

This shall be the name commercially used by the CSP to designate the cloud service. The name shall include enough information, such as qualifiers, version names or numbers, to unambiguously identify the cloud service.

<SHORT DESCRIPTION>

This shall be a description of the functionality of the cloud service]

<ASSURANCE LEVEL>

This is the assurance level for which the CSP applies for certification; its value shall be one of Basic, Substantial or High.

For the appropriate choice refer to the description of the assurance levels.

<SECURITY PROFILES>

This shall be the list of the security profiles applicable to the cloud service, including for every security profile its full name, reference number, version number and date of issuance.

Security profiles define additional requirements that are specific to an industry or vertical application. The reference list of valid security profiles is maintained by ENISA.

<APPLICATION TYPE>

This is the type of conformity assessment to be performed; its value shall be one of 'initial', 'periodic', 'renewal' or 'restoration'.

For Application Types 'periodic', 'renewal' and 'restoration', additional information is required in the description of the service.

<APPLICATION PERIOD>

When applicable (levels Substantial and High), this shall be the period that the CAB will consider in the assessment of operational effectiveness.

This period depends on the date of the last assessment, and it typically will be one year. For initial assessments, there are minimum values depending on the assurance level.

F.2.2 CSP's Management Statement

<MANAGEMENT STATEMENT>

This is the management state of the CSP, which shall be dated and signed, and which shall at least point out that:

- the documentation filed for certification is complete;
- this documentation is accurate and up-to-date;
- this documentation meets the requirements for certification in the EUCS scheme; and
- this documentation is a true reflection of the processes, procedures and systems in place within the organisation in scope of the certification;
- the organisation and its management are committed to comply with all their obligations during the conformity assessment and after certification during the entire lifecycle of their cloud service's certificate;
- the management of the applying organisation declares to be responsible for the abovementioned points;
- the management of the applying organisation declares to fully cooperate and be transparent to the extent needed to handle the complaints in the procedure for complaints ex Art. 63 of the EUCSA;
- the management of the applying organisation declares that it is providing full cooperation in investigative activities of the NCCA ex Art. 58(8) of the EUCSA;
- the management of the applying organisation declares that it is authorising and approving to cooperate in compliance audits of the certification issuing body and applicable peer reviews ex Art. 59 of the EUCSA, and if applying for assurance level 'high' to peer assessments as defined in the EUCS scheme ex Art 54(1)(u).

F.2.3 CSP's Description of its service

<SERVICE DESCRIPTION>

There is no mandatory content for the item <SERVICE DESCRIPTION>. This item is also the identifier for the information in the items of this section.

The CSP may include some guidance to help the reader through the rest of the section.

F.2.3.1 The types of services provided

<TYPES OF SERVICES>

The <TYPES OF SERVICES> item shall describe the specific functional purposes of the Cloud Service.

The cloud service (singular) for which the evaluation is requested may offer multiple (plural) functional services. For example a cloud service 'communications' could have functional types of services such as Email, Voice, and Video calling.

F.2.3.2 The components of the system

<SERVICE COMPONENTS>

There is no mandatory text for the CSP to provide for the item <Service Components>. This item is the identifier for the information in the items of this paragraph.

<PHYSICAL INFRASTRUCTURE>

This item lists the physical components that are relevant to the make up the Cloud Service. The CSP shall provide reference to relevant underlying documentation and procedures.

Examples of Physical Infrastructure are datacentres, equipment, and telecommunication networks.

<SOFTWARE>

This item lists the relevant software application programs and system software underlying the cloud service.

Examples of Software are operating systems, middleware, and utilities.

<PEOPLE>

This item lists the CSP personnel relevant to the governance, operation, and usage of the cloud service.

Examples of roles mentioned in <PEOPLE> are developers, operators, users, and managers.

<POLICIES AND PROCEDURES>

This item lists the policies and the automated and manual procedures relevant to the CSP's operation of the cloud service.

<DATA>

Where applicable, this item lists the data the CSP requires to operate the Cloud Service.

Examples of Data are transaction streams, files, databases and tables.

F.2.3.3 *The boundaries or aspects of the system covered by the description*

<SERVICE BOUNDARIES>

The <Service Boundaries> shall describe the boundaries of the system under certification.

There is no specific mandated format for the description, but it should be sufficient for the CAB to understand precisely the scope of the conformity assessment to be performed.

F.2.3.4 *Subservices*

<SUB SERVICES>

The item <SUB SERVICES> lists all the sub services that are material to the operation of the cloud service. For each subservice organization the CSP shall provide:

- the role of the subservice
- the sub service organization
- the type and scope of functions and services provided
- the EUCS requirements that apply to that subservice organisation
- the Complementary subservice organization controls (CSOCs) applicable to the subservice organization
- assurance the sub service adheres to appropriate controls of the Scheme
- assurance on the CSP responsibility over adherence of the subservice

The assurance may be provided by listing industry certifications relevant and valid for the Assurance Level and Application Period of certification of the cloud service.

F.2.3.5 *Information for customers*

The information in this section is mandatory information to be made available to customers.

The current version only lists the information available, but it is likely to be enriched with a mandatory presentation of the information, in order to ease the comparison between cloud services.

<SUPPLEMENTARY INFORMATION>

This item shall include a list of the supplementary information to be made publicly available by the CSP in application of Art. 54(1)(v) of the EUCSA.

The CSP should include pointers to the various elements to be provided, as well as a short rationale explaining why they meet the requirements. As required by the EUCSA, this information will be made public on ENISA's website, together with the certificate and the information about the certified service.

<TRANSPARENCY INFORMATION>

This item shall include comprehensible and transparent information on the CSP's:

- Jurisdiction; and
- Locations where the cloud customer's data is processed, stored, and backed up, including the CSP's own locations and the locations of all other service providers supporting the provision of the service.

The information provided shall be compliant to all the requirements of objective DOC-03 that are relevant to the targeted assurance level.

<COMPLEMENTARY CUSTOMER CONTROLS, CCC>

This item shall list all relevant Complementary Customer Controls (CCC) contemplated in the design of the CSP Cloud Service, and those CCCs that are relevant to a Cloud Service user's operation of the Cloud Service in accordance with the scheme security requirement.

This item shall include a complete list of the CCCs listed per requirement in the Control Objectives.

F.2.3.6 Maintenance information

<MAINTENANCE INFORMATION>

The section is required for application types periodic', 'renewal' and 'restoration'. There is no mandatory content for the item <MAINTENANCE INFORMATION>. This item is also the identifier for the information in the items of this section.

The CSP may include some guidance to help the reader through the rest of the section.

<CHANGES IN THE CLOUD SERVICE>

This item shall list all the changes in the definition and operation of the Cloud Service and of its supporting organization since the last security assessment performed on the Cloud Service.

The list may reference the controls listed in the following section.

<IMPACT ANALYSIS>

This item shall list all the EUCS requirements that may be affected by the changes listed in <CHANGES IN THE CLOUD SERVICE>.

The information provided in this list, together with the description in <CHANGES IN THE CLOUD SERVICE>, should allow the CAB to determine the list of conformity assessment activities that need to be performed regarding these changes.

<NONCONFORMITIES TO BE ADDRESSED>

This item is required for application type 'restoration' only. It shall contain a list of the nonconformities that need to be addressed, including at least for each nonconformity:

- The requirement on which the nonconformities has been identified;
- The severity of the nonconformity ('minor' or 'major');
- A short description of the nonconformity.

This is strongly related to the <CHANGES IN THE CLOUD SERVICE> and <IMPACT ANALYSIS>, since the requirements listed here should also appear in the <IMPACT ANALYSIS> to indicate that the <CHANGES IN THE CLOUD SERVICE> have addressed the issues.

F.2.3.7 Other

<OTHER INFORMATION>

This optional item may be used by the CSP to provide other information the CSP considers relevant in context of the certification evaluation of its cloud service.

F.2.4 The security objectives and CSPs description of controls

<CONTROL OBJECTIVES>

The item <CONTROL OBJECTIVES> shall define how the security controls defined and implemented by CSP meet the security requirements defined in the EUCS scheme. For each security requirement, the information shall include:

- If the security requirement is not applicable to the Cloud Service, an indication of this non-applicability, together with a rationale.
- Otherwise, a list of the following controls, together with a description:
 - security controls that contribute to meeting of the security requirement;
 - Complementary Sub-service Organization Controls (CSOCs); and
 - Complementary Customer Controls (CCCs)

The content of the <CONTROL OBJECTIVES> shall be organized in a table following the template shown below:

Security Control Objectives and related Security Requirements of the EUCS	<CSP>'s Description of Controls, assumed CSOCs and CCCs, or Rationale if Security Requirement is not applicable
Security Control Objective: [...].	
ID – Title of Security Requirement [Description of the Security Requirement]	ID – Title of Control 1 to meet the Security Requirement or Rationale if Security Requirement is not applicable [Control Description/Rationale]
	ID – Title of Control 2 to meet the Security Requirement [Control Description]
	CSOCs: [CSOC Description] / none CCCs: [CCC Description] / none

F.3 AUDIT PLANNING

F.3.1 Initial activities planning

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the recommendations for the “Initial activities planning and execution” document.

This document is an internal to the CAB. It may be part of the documentation provided by the auditor in addition to the evaluation report for the review phase. The CAB is free to modify the format, but the elements of information are important to

A CAB should apply these recommendations in its description of the initial audit activities to be performed as a preparation to the detailed audit planning, and in its reporting of these initial activities.

Mandatory field in the template	Clarification
Section 1: “ Activities ” This section describes the initial activities of the audit. The items described below shall be filled out for every initial audit activity relevant for the targeted assurance level.	
Objective	Objective of the activity
Information and documentation used	Information used in support of the activity
Evidence gained	Evidence
Conclusion reached	Conclusion for the activity
Date	Date of the conclusion
Initials	Initials or signature of the auditor

CONTENT OF THE DOCUMENT

F.3.1.1 *Activities*

The items listed below are recommended for the description of one activity, so they should be repeated for each activity described.

<OBJECTIVE>

The CAB should include the objective of the activity, as listed in the assessment requirements.

<INFORMATION AND DOCUMENTATION USED>

The CAB should list the documentation on which the activity was based (from the documentation provided by the CSP in the application document and in support of the application).

<EVIDENCE GAINED>

The CAB should describe the evidence gained from the activity.

<CONCLUSION REACHED>

The CAB should describe the conclusion reached for the activity.

The conclusions are expected to lead to easier

<DATE>

The CAB should indicate the date when the conclusion for the activity was documented.

<INITIALS>

The audit team member who performed the activity should initial the document in a way that unambiguously identifies the member within the audit team.

F.3.2 Detailed audit plan and execution

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Detailed audit plan and execution” document for any assessment performed at level Substantial or High.

A CAB should apply these requirements in two phases:

- during its description of detailed audit activities;
- during the execution of the audit.

Mandatory field in the template	Clarification
Section 1: “ Audit activities ” This section describes the activities of the audit. The items described below shall be filled out for every security objective relevant for the targeted assurance level.	
EUCS objective	The security objective and reference from EUCS
1.1 Procedures	
Procedure re Suitability	Information used in support of the activity
- Nature	Nature of the activity
- Timing	Timing of the activity
- Extent	Extent of the activity
Procedure re Existence	Audit activities to be performed
- Nature	Nature of the activity
- Timing	Timing of the activity
- Extent	Extent of the activity
Procedure re Operating Effectiveness	Conclusion for the activity
- Nature	Nature of the activity
- Timing	Timing of the activity
- Extent	Extent of the activity, including sampling
1.2 Execution	
Sources	Information used and people inquired in support of the activity
Evidence gained	Evidence
Conclusion reached	Conclusion for the activity
Date	Date of the conclusion
Initials	Initials or signature of the auditor

CONTENT OF THE DOCUMENT

F.3.2.1 Characteristics of an audit activity

The document consists of descriptions of procedures to be applied to audit how the cloud service fulfils the EUCS objectives and requirements. Each audit activity should be described with the following parameters:

<NATURE>

The kind of audit activity to be performed, together with a description of the activity

<TIMING>

The timing of the activity, either as a point of time, or as a period to be covered

<EXTENT>

The extent of the activity, *i.e.*, the number of times the activity needs to be performed, including a rationale if sampling is used

F.3.2.2 Procedures

The items listed below are recommended for the description of the procedures related to one security objective, so they should be repeated for each security objective described.

<EUCS OBJECTIVE>

The CAB should include the objective of the activity, as listed in the assessment requirements, including the reference from EUCS.

<PROCEDURE RE SUITABILITY>

The procedure to be executed for auditing the suitability of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

<PROCEDURE RE EXISTENCE>

The procedure to be executed for auditing the existence of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

<PROCEDURE RE OPERATING EFFECTIVENESS>

The procedure to be executed for auditing the operating effectiveness of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

F.3.2.3 Execution

This section describes the execution of the audit activities and the results achieved, including a conclusion about the fulfilment of the EUCS requirements related to the security objective.

<SOURCES>

Information used and people inquired in support of the activities related to the objective.

<EVIDENCE GAINED>

Evidence that has been gained in the activities related to the objective.

<CONCLUSION REACHED>

Conclusion reached regarding the fulfilment of the objective and related requirements by the cloud service.

<DATE>

Date of the conclusion.

<INITIALS>

Initials of the auditor in charge of the activities.

F.4 ASSURANCE AND EVALUATION REPORT

The evaluation phase results in two reports:

- The assurance report resulting from the audit of the CSP;
- The evaluation report that contains the dependency analysis (if required), together with the final recommendation from the evaluation;

F.4.1 Assurance report

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the "Assurance report" document.

The assurance report is the report from the audit activity, which is then completed by the evaluation report. The assurance report shall contain a detailed report of the conformity assessment activities performed by the CAB toward demonstrating that the assessed cloud service meets the requirements of the scheme. The assurance report shall in addition include a recommendation regarding the certification of the assessed cloud service.

A CAB shall apply these requirements when preparing the report at the end of the audit of the cloud service.

Mandatory field in the template	Clarification
Section 1: "Identification" This section identifies the conformity assessment body in charge of the certification, and the cloud service being audited.	
1.1 CAB	
CAB identity	Identify of the CAB in charge of the certification
CAB contact	Identification and contact details for the lead contact at the CAB that will manage the evaluation process
Accreditation details	Details about the ability of the CAB to perform an audit
Lead auditor	Affiliation, contact information and qualification of the lead auditor
Audit team	Affiliation, contact information and qualification of the audit team members
1.3 CSP	
CSP identity	Identity of the CSP requesting the evaluation.
CSP contact	Identification and contact details for the lead contact at the CSP that will support the evaluation process
1.4 Cloud service	
Service Name	Commercial name of the CSP Cloud Service for which the evaluation is requested
Short Description	A short description of the functionality of 'Service Name'.
Assurance Level	The assurance level for which the evaluation is requested. Valid values are Basic, Substantial and High
Security Profiles	The list of security profiles applicable to the cloud service
Application Type	CSP specified evaluation application type. Valid values are 'initial', 'periodic', 'renewal' or 'restoration'.
Application Period	When applicable, the period to be considered by the CAB for the assessment of operational effectiveness.
Application Number	The registration number assigned to the Application document upon receipt by the CAB

Mandatory field in the template	Clarification
Section 2: "CSP's Claim" This section is the CSP's management assertion the template accurately and fairly describes the Cloud Service and the applicable controls from the scheme's framework.	
From the Application document	
Section 3: "CSP's Description of its service" This section is the CSP's assessment of the Cloud Service's implementation of the scheme's requirements and control framework.	
Description	From the application document
Self-Assessment	Assessment of the conformity to EUCS requirements (Basic assurance level only)
Section 4: "CAB's Responsibility Assertion" This section is the CAB's management assertion about their responsibility.	
Responsibility	Statement from the CAB
Scope	Scope of the audit (including references to the CSP's description and to the CAB's activities)
Disclaimers	Standard disclaimers about the audit activities
Section 5: "CAB's Audit Activities and Results" This section describes the CAB's audit activities and results.	
4,1 Presentation	
4.2 Audit activities and results	
Reasonable assurance	Description and results of the audit activities (version for the Substantial and High levels)
Limited assurance	Description and results of the audit activities (version for the Basic level)
4.3 Nonconformities	
Requirement reference	Reference of the EUCS security objective and requirement for which a nonconformity has been identified
Nonconformity	Description of the nonconformity
Severity	The severity of the nonconformity, which may be 'minor' or 'major'
Suitability of mitigation	The analysis of the mitigation proposed by the CSP
Section 6: "CAB's conclusion" This section describes the conclusion of the CAB's audit regarding the suitability of the cloud service for certification	
Conclusion	Conclusion about the fulfillment of EUCS requirements by the cloud service
Disclaimer	A disclaimer indicating that the conclusion needs to be combined with the conclusion of the evaluation report.

CONTENT OF THE DOCUMENT

F.4.1.1 Identification

Identification of the CAB

<CAB IDENTITY>

The legal identity of the organisation issuing the report shall be provided, including at least:

- Legal name of the organization;
- Registration number in Chamber of Commerce or equivalent; and
- Office and headquarter location;

If the organization operates as a subcontractor for another CAB that will issue the certificate, the same information shall be provided about that other CAB.

<CAB CONTACT>

The contact details of the responsible department and of the person that is legally representing the organization for the purpose of that audit shall be provided

<ACCREDITATION DETAILS>

The CAB in charge of the conformity assessment shall include the information related to its ability to perform an audit:

- Accreditation number and notification number and contact details of issuing body;
- If assurance level High is applicable, and Article 56(6) applies, a signed statement of the NCCA authorizing the CAB to perform the conformity assessment;

If the organisation issuing the report is a subcontractor of the CAB and has obtained a separate accreditation to perform audit work, then they shall provide the following information:

- Accreditation number and notification number;

<LEAD AUDITOR>

The affiliation, contact information and qualification of the lead auditor shall be provided.

<AUDIT TEAM>

The affiliation, contact information, role and qualification of every member of the audit team shall be provided.

Identification of the CSP

<CSP IDENTITY>

This item shall include the content of the <CSP IDENTITY> item from the Application Document.

<CSP CONTACT>

This item shall include the content of the <CSP CONTACT> item from the Application Document.

Identification of the cloud service

<SERVICE NAME>

This item shall include the content of the <SERVICE NAME> item from the Application Document.

<SHORT DESCRIPTION>

This item shall include the content of the <SHORT DESCRIPTION> item from the Application Document.

<ASSURANCE LEVEL>

This item shall include the content of the <ASSURANCE LEVEL> item from the Application Document.

<SECURITY PROFILES>

This item shall include the content of the <SECURITY PROFILES> item from the Application Document.

<APPLICATION TYPE>

This item shall include the content of the <APPLICATION TYPE> item from the Application Document.

<APPLICATION PERIOD>

This item shall include the content of the <APPLICATION PERIOD> item from the Application Document.

<APPLICATION NUMBER>

This item shall contain the application number issued by the CAB upon reception of the Application Document.

F.4.1.2 CSP's claim

This section shall contain the CSP's claim from the Application Document.

F.4.1.3 CSP's description of its service

This section contains the information provided by the CSP about its cloud service.

<DESCRIPTION>

The description of the service provided by the CSP in the Application Document.

<SELF-ASSESSMENT>

This item is only relevant for assurance level Basic.

This item shall include the self-assessment provided by the CSP following the template provided by the CAB.

F.4.1.4 CAB's responsibility assertion

This section is the CAB's assertion of their responsibility and to its compliance to the scheme, which shall be dated and signed.

<RESPONSIBILITY>

The CAB in charge of the conformity assessment shall include the information related to its responsibility in the audit:

- A declaration of independence and quality control; and
- A declaration of protection of information (confidentiality obligations and IP obligations).

If the organisation issuing the report is a subcontractor of the CAB, then they shall provide the following information:

- A declaration of independence and quality control; and
- A declaration of protection of information (confidentiality obligations and IP obligations).

In all cases, the organisation issuing the report shall also include a declaration of evaluation according to the applicable rules, stating that the conformity assessment activities described in the report were performed in accordance with the requirements of the EU Cybersecurity Act, of the EUCS scheme and, if applicable, to authorisation requirements defined by the NCCA.

<SCOPE>

Based on the information provided earlier in the document, a short statement of what has been evaluated shall be provided:

- Overview of the reviewed documentation,
- List of on-site visits;
- Overview of the testing performed; and
- List of persons interviewed.

The definition of the scope shall be a short summary, without the details provided in the description of the CAB's audit activities.

<DISCLAIMERS>

The assurance report shall include disclaimers that convey the information that:

- No certification can lead to a 100% security guarantee, but only to a reasonable certainty that the level of security is meeting the requirements for the assurance level at the moment of certification and during the certification lifecycle;
- Security controls are evaluated to the best of abilities, required skills and knowledge of the evaluating parties; and

- There is no guarantee that certification excludes all forms of fraud, misleading or circumvention of controls but the EUCS scheme is aiming to prevent such fraudulent behaviour as much as possible.

F.4.1.5 CAB's audit activities and results

Presentation

<PRESENTATION>

This item is optional. The CAB may include a presentation of the audit activities.

Audit activities and results

This section shall contain one of the two subsections listed below, depending on the assurance level of the conformity assessment.

F.4.1.6 Limited assurance

This section only applies to assurance level Basic.

This section is **to be defined**.

F.4.1.7 Reasonable assurance

This section only applies to assurance level Substantial and High.

The CAB shall provide the following table, which presents the CAB's test procedures and results per control.

<CSP>'s Description of Controls	Applicable EUCS requirements	<CAB>'s Audit Activities and Results
ID – Title of Control [Control Description]	Ref. 1 Ref. 2 Ref. 3	Inquired the [...] <i>No nonconformities identified</i> Inspected [...] <i>No nonconformities identified</i>
ID – Title of Control [Control Description]	Ref. 1 Ref. 2 Ref. 3	Inquired the [...] <i>No nonconformities identified</i> Inspected [...] <i>No nonconformities identified</i>

Note that the example provided above indicates "No nonconformities identified". In case a nonconformity is identified, it shall be noted, with a reference to the nonconformity's description in the following section.

Nonconformities

This section shall list all the nonconformities identified during the audit, including a summary of the analysis of the analysis performed by the CAB of the nonconformity and of the mitigation proposed by the CSP.

<REQUIREMENT REFERENCE>

This item shall include a reference to the objectives and requirements that are not being fulfilled.

<NONCONFORMITY>

This item shall include a description of the nonconformity.

In the case of multiple nonconformities related to the same requirement, the description shall include enough information to support the analysis of the nonconformity's severity.

<SEVERITY>

This item shall include a summary of the analysis performed by the CAB to determine the severity of the nonconformity, as well as the conclusion (minor or major nonconformity).

<SUITABILITY OF MITIGATION>

This item shall include a summary of the analysis performed by the CAB to determine the suitability of the mitigation proposed by the CSP.

For a minor nonconformity, a simple analysis of the proposed mitigation actions or compensating controls is sufficient. For a major nonconformity, the mitigations shall be implemented, and the analysis shall point to audit activities that verifies the success of the mitigation.

Note that the mitigation of a major nonconformity is considered successful if it leads to no nonconformity or to a minor nonconformity. In the case of a minor nonconformity, it is also listed in the section.

F.4.1.8 CAB's conclusion

This section is the conclusion about the fulfilment of EUCS requirements by the cloud service, to the extent determined by the audit, which shall be dated and signed by the lead auditor.

<CONCLUSION>

This is the conclusion of the lead auditor regarding the audit.

The conclusion can only be partial, since it will depend on the dependency analysis. More details need to be added.

<DISCLAIMERS>

TO BE DEFINED

A disclaimer will need to be added to indicate that the fulfilment of the EUCS requirements also depend on the dependency analysis, to be performed independently.

F.4.2 Evaluation report

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the "Evaluation report" document.

A CAB shall apply these requirements when preparing the report at the end of the audit of the cloud service.

Mandatory field in the template	Clarification
<p>Section 1: "Identification"</p> <p>This section identifies the conformity assessment body in charge of the certification, the audit team in charge of the assurance report, and the cloud service being audited.</p> <p>Same as for the Assurance Report</p>	
<p>Section 2: "CSP's Claim"</p> <p>This section is the CSP's management assertion the template accurately and fairly describes the Cloud Service and the applicable controls from the scheme's framework.</p> <p>From the Application document</p>	
<p>Section 3: "CSP's Description of its service's dependencies"</p> <p>This section is the CSP's assessment of the cloud service's dependencies towards subservice organizations, together with a list of the available assurance documentation for these services.</p>	
Description	From the application document
Self-Assessment	Assessment of the conformity to EUCS requirements (Basic assurance level only)
<p>Section 4: "CAB's Responsibility Assertion"</p> <p>This section is the CAB's management assertion about their responsibility.</p> <p>Same as for the Assurance Report</p>	
<p>Section 5: "CAB's Dependency Analysis Activities and Results"</p> <p>This section describes the CAB's dependency analysis activities and results.</p>	
5,1 Presentation	An optional presentation of the activities
5.2 Activities and results	
Reasonable assurance	Description and results of the audit activities (version for the Substantial and High levels)
- Assurance documentation	Verification of the suitability of the nature of documentation available, of the framework used, of the conclusions, and other relevant criteria
- Documentation origin	Verification of the origin of the documentation (CAB, auditor), guarantees about competence and independence
- Scoping	Verification of the scope of the documentation with respect to the scope expected by the CSP (covering both dimensions: functionality and security requirements)
- Nonconformities	Analysis of the nonconformities indicated in the assurance documentation that may affect the decision
- Analysis	Combined analysis of all the results regarding the subservice provider
Limited assurance	Description and results of the audit activities (version for the Basic level)
5.3 Nonconformities	
Requirement reference	Reference of the requirement that is not being fulfilled (which may also be a CSOC)
Nonconformity	Description of the nonconformity
Severity	Severity of the nonconformity
Suitability of mitigation	Overview of the proposed mitigation and of its suitability to address the nonconformity

Mandatory field in the template	Clarification
Section 6: " CAB's conclusion " This section describes the conclusion of the CAB's audit regarding the suitability of the cloud service for certification	
Dependency Conclusion	The conclusion of the dependency analysis
Recommendation	Combined conclusion of audit and dependency analysis and recommendation for the certification decision

CONTENT OF THE DOCUMENT

F.4.2.1 *Identification*

This section has the same content as the one described in the Assurance Report (F.4.1.1)

F.4.2.2 *CSP's claim*

This section shall contain the CSP's claim from the Application Document.

F.4.2.3 *CSP's description of its service's dependencies*

<DESCRIPTION>

This item shall contain the content of the <SUB SERVICES> item from the Application Document (F.2.3.4).

<Self-Assessment>

This item is only relevant for assurance level Basic.

This item shall include the self-assessment provided by the CSP following the template provided by the CAB for assessing the adequacy of the assurance documentation available and the sufficiency of the controls covered by that assurance documentation.

F.4.2.4 *CAB's responsibility assertion*

This section has the same content as the one described in the Assurance Report (F.4.1.4)

F.4.2.5 *CAB's dependency analysis activities and results*

Presentation

<PRESENTATION>

This item is optional. The CAB may include a presentation of the audit activities.

Audit activities and results

This section shall contain one of the two subsections listed below, depending on the assurance level of the conformity assessment.

LIMITED ASSURANCE

This section only applies to assurance level Basic.

This section is to be defined.

REASONABLE ASSURANCE

This section only applies to assurance level Substantial and High.

The CAB shall provide the following information, which presents the CAB's dependency analysis activities and results.

The items below need to be replicated for every subservice provider.

<ASSURANCE DOCUMENTATION>

This item shall include a description of the nature of the documentation followed by an analysis of its suitability. The following elements shall be considered:

- Nature of the documentation (ISAE report, certificate, other) and type (ISAE report type, certification scheme);
- Period covered, certificate validity;
- Applicable framework and availability/sufficiency of mapping to EUCS requirements;
- Sufficiency of the report for understanding the subservice organization's controls.

If the assurance documentation is an EUCS certificate, then checks are only required of the certificate validity and of the assurance level.

More information about acceptable reports and certificates and specific attention points for every type of report will be provided as guidance.

<Documentation Origin>

This item shall include a description of the organization who issued the report or certificate, followed by an analysis of its suitability. The following elements shall be considered:

- Identity of the issuing organization and, if required of the lead auditor;
- Competence of the issuing organization and lead auditor (accreditation, personal certification);
- Independence of the issuing organization and lead auditor (accreditation, other indication)

If the assurance documentation is an EUCS certificate, then no checks are required.

<SCOPING>

This item shall include a description of the scope of the assurance documentation, followed by an analysis of its suitability with regard to the requirements (EUCS requirements, CSOCs) described by the CSP. The following elements shall be considered:

- Systems and locations in scope that are relevant for the CSP;
- Applications and services that are relevant to the CSP;
- Carved-out components and other subservice providers;
- Sufficiency of the scope to cover the requirements of the CSP, including CSOCs.

If the assurance documentation is an EUCS certificate, then subservice providers do not need to be identified.

<NONCONFORMITIES>

This item shall include a description of the nonconformities identified in the assurance documentation, followed by an analysis of their impact. The following elements shall be considered:

- Nonconformities or deviations identified in the assurance documentation that may affect the CSP;
- Severity or qualification of the nonconformities or deviations;
- Description of proposed mitigation and opinion of the auditor.

<ANALYSIS>

This item shall include an analysis that considers together all the activities described above in order to reach a conclusion about the suitability and sufficiency of the assurance documentation available for the subservice provider.

Nonconformities

This section shall list all the nonconformities identified during the audit, including a summary of the analysis of the analysis performed by the CAB of the nonconformity and of the mitigation proposed by the CSP.

<REQUIREMENT REFERENCE>

This item shall include a reference to the objectives and requirements that are not being fulfilled.

This item may refer to an EUCS requirement or to a CSCO defined by the CSP.

<NONCONFORMITY>

This item shall include a description of the nonconformity.

In the case of multiple nonconformities related to the same requirement, the description shall include enough information to support the analysis of the nonconformity's severity.

The nonconformity is not necessarily linked to a nonconformity identified in assurance documentation, as it may relate to any part of the dependency analysis.

<SEVERITY>

This item shall include a summary of the analysis performed by the CAB to determine the severity of the nonconformity, as well as the conclusion (minor or major nonconformity).

<SUITABILITY OF MITIGATION>

This item shall include a summary of the analysis performed by the CAB to determine the suitability of the mitigation proposed by the CSP.

For a minor nonconformity, a simple analysis of the proposed mitigation actions or compensating controls is sufficient. For a major nonconformity, the mitigations shall be implemented, and the analysis shall point to audit activities that verifies the success of the mitigation.

Note that the mitigation of a major nonconformity is considered successful if it leads to no nonconformity or to a minor nonconformity. In the case of a minor nonconformity, it is also listed in the section.

F.4.2.6 CAB's conclusion

This section is the conclusion about the fulfilment of EUCS requirements by the cloud service, to the extent determined by the audit, which shall be dated and signed by the lead auditor.

<DEPENDENCY CONCLUSION>

This is the conclusion of the lead auditor regarding the dependency analysis, considering all subservice providers.

<RECOMMENDATION>

This item shall include the final recommendation of the auditor, based on the conclusion of the Assurance Report and the conclusion of the dependency analysis. The auditor shall determine whether or not the cloud service meets the EUCS requirements for the targeted assurance level, and shall provide a recommendation regarding the certification of the cloud service.

The recommendation shall be dated and signed by the lead auditor.

F.5 REVIEW REPORT

This is an internal document, generated during the review phase, in which the reviewer records the result of its review of the audit.

A template will be provided later for guidance.

F.6 CERTIFICATE PACKAGE

F.6.1 Certificate

The template for certificates will be defined later.

F.6.2 Certification report

PRESENTATION

The paragraph ‘Content of the document’ in this section defines the requirements for the “Evaluation report” document.

A CAB shall apply these requirements when preparing the certification report that accompanies the certificate.

This document is part of the certificate package, and it is publicly available from CAB’s and from ENISA’s web sites. It contains the information made publicly available about the cloud service and about the result of the conformity assessment.

Note that the requirements on this document are likely to be strengthened in the future, in order to move as much as possible to a standardized format that simplifies the comparison of certified cloud services.

Mandatory field in the template	Clarification
Section 1: “Independent Conformity Assessment Body report” This section confirms the evaluation work done by the CAB.	
Scope	Description of the scope of the evaluation
CSP Management Responsibilities	Description by the CAB of the CSP’s management responsibilities in the evaluation
CAB responsibilities	Description by the CAB of the CAB’s responsibilities in the evaluation and of the inherent limitations of the evaluation
Certification decision	Description by the CAB of the outcome of the evaluation, which led to the positive certification decision
Section 2: “Management’s report” This section is the CSP’s management confirmation of its responsibilities and assertion of the effectiveness of the implemented controls in relation to the EUCS scheme’s requirements.	
CSP Management Statement	A written conformity statement by the management of the CSP
Section 3: “Cloud service scope” This section is the CSP’s assessment of the cloud service’s implementation of the scheme’s requirements.	
Background	Information on the CSP as an organization
Cloud service	The cloud service in scope for the evaluation, including the commercial names used for the cloud service.
Service components	A list of the main components of the cloud service
Section 4: “Principle Service Commitments and System Requirements” Description of the cloud service, the CSP commitments and requirements.	
Description	General description provided by the SP of its approach to cybersecurity assurance and compliance to the scheme
a) Physical Infrastructure	Description of physical structures at the CSP that make up the cloud service.
b) People	Description of (types of) personnel at the CSP involved in the governance and operation of the cloud service
c) Procedures	Description of automated and manual procedures at the CSP involved in the governance and operation of the cloud service

Mandatory field in the template	Clarification
d) Data	Description of the data involved in the governance, operation, and use of the cloud service.
e) Confidentiality	Description by the CSP of the measures that support confidentiality in relation to the cloud service
f) Integrity	Description by the CSP of the measures that support integrity in relation to the cloud service
g) Availability	Description by the CSP of the measures that support availability in relation to the cloud service
Section 5: “Additional information” This section includes the information required as to be transparent in the part of the EUCS scheme.	
Supplementary information	The information that has to be made available by the Cybersecurity Act's article 55
Location and legal information	Information about the location of the storage and processing of customer data, and about applicable laws.

CONTENT OF THE DOCUMENT

F.6.2.1 *Independent Conformity Assessment Report*

<SCOPE>

This item shall contain a description of the scope of the evaluation, including at least:

- The targeted assurance level
- If applicable, the list of claimed security profiles
- A high-level description of the certified cloud service

<CSP MANAGEMENT RESPONSIBILITIES>

This item shall contain a description of the CAB’s understanding of the CSP’s responsibilities, drawn from the CSP management’s statement including in the Application Document.

<CAB RESPONSIBILITIES>

This item shall contain a description of the CAB’s own responsibilities, matching the statement provided in the other reports, and in particular in the Assurance Report and Evaluation Report.

<CERTIFICATION DECISION>

This item shall contain a description of the CAB’s certification decision, including at least

- A statement about how CAB has verified that the cloud service meets the EUCS scheme’s requirements
- An overview of the subservices and how they have been considered to contribute meeting the EUCS scheme’s requirements
- An overview of the nonconformities and how the proposed mitigations have been determined appropriate

F.6.2.2 *Management’s report*

<CSP MANAGEMENT STATEMENT>

This item shall contain a CSP management statement drawn from the statement provided in the Application Document.

F.6.2.3 *Cloud service scope*

<BACKGROUND>

This item shall contain information about the CSP as an organization and their commitment to cybersecurity.

<CLOUD SERVICE>

This item shall include an overview of the cloud service that is in scope for the certification, including the commercial names and the corresponding functions.

<SERVICE COMPONENTS>

This item shall include a description of the main components used for the development and operation of the cloud service.

F.6.2.4 Principle service commitments and system requirements

<DESCRIPTION>

This item shall include a general description provided by the CSP of its approach to cybersecurity assurance and compliance to the requirements of the EUCS scheme.

<PHYSICAL INFRASTRUCTURE>

This item shall include a description of the physical structures at the CSP that are used to develop, provide and support the cloud service.

<PEOPLE>

The item shall include a description of the personnel (categories) and key roles at the CSP who are involved in the development, governance and provision of the cloud service.

<PROCEDURES>

This item shall include a description of the automated and manual procedures at the CSP that are involved in the development, governance and provision of the cloud service.

<DATA>

This item shall include a description of the data involved in the governance, operation and use of the cloud service.

<CONFIDENTIALITY>

This item shall include a description of the measures implemented by the CSP to support confidentiality in relation to the cloud service.

<INTEGRITY>

This item shall include a description of the measures implemented by the CSP to support integrity in relation to the cloud service.

<AVAILABILITY>

This item shall include a description of the measures implemented by the CSP to support availability in relation to the cloud service.

F.6.2.5 Other information

This section is optional.

<OTHER INFORMATION>

If present, this item shall include additional information that the CSP considers relevant in context of the certification of its cloud service.

Note that the information provide in this section needs to be accepted and reviewed by the CAB, like all information in the report.

F.7 MAINTENANCE REPORTS

F.7.1 Impact analysis report

In some cases, the monitoring activities will lead to requests regarding potential nonconformities or vulnerabilities that will not lead to a conformity assessment. This report would outline the answer from the SP and the analysis from the CAB.

F.7.2 Maintenance report

The need for a maintenance report is still under discussion. A maintenance report would be a version of the certification report tailored for maintenance assessments. In particular, it would focus on the changes since the last report, to make the crucial information more easily accessible to scheme users.

ANNEX G: CERTIFICATION LIFECYCLE AND CONTINUED ASSURANCE

PURPOSE	This annex describes additional content related to the chapters on certification lifecycle and continued assurance
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 11, Compliance Monitoring Chapter 12, Certificate Management Chapter 13, Non-Compliance Chapter 14, New Vulnerabilities

Foreword for Reviewers

This Annex is work in progress; its content is not final, and it is only intended to provide an overview of the planned processes for the different types of conformity assessment needed.

It has not yet reviewed by the TG3 and TG5 thematic group.

G.1 ASSESSMENT DURING MAINTENANCE

The initial conformity assessment of a cloud service shall cover all parts of the assessment methods defined in Annex B: (Meta-approach for the assessment of cloud services), Annex C: (Assessment for levels Substantial and High), Annex D: (Assessment for level Basic) for all EUCS requirements defined in Annex A: (Security Objectives and requirements for Cloud Services).

However, during maintenance some conformity assessments may be simplified, provided that they follow the minimum requirements defined below.

G.1.1 Periodic assessment

In a periodic assessment, the conformity assessment shall include at least the following activities.

Analysis of the change in the cloud service

These activities are required at all assurance levels.

The CAB shall at least:

- Obtain an understanding of the changes operated since the last assessment in the cloud service and the CSP's controls to meet the Security Objectives and related Security Requirements;
- Determine a list of affected controls, based on the CSP's Impact Assessment and if needed on additional inquiries;
- Assess the suitability of the design of the modified controls.
- Assess the existence and implementation of the modified controls.

Partial reassessment of controls

These activities are only required at assurance levels Substantial and High.

The CAB shall at least:

- Select a subset of controls, including at least the controls for which nonconformities have been detected in the previous assessment and controls defined in a dedicated guidance to be provided on a regular basis by ENISA with the support of the ECCG.
- Assess the suitability of the design of the modified controls.

Effectiveness assessment

These activities are only required at assurance levels Substantial and High.

The CAB shall at least:

- Assess the operating effectiveness of all controls over the period since the previous assessment of operating effectiveness.

If some controls have been affected by the changes in the cloud service since the last assessment and if they have been operating for less than 3 months (6 months for level High), the CAB shall assess to which extent of the changes affect their ability to assess the operating effectiveness of the controls.

G.1.2 Renewal assessment

Alike an initial assessment, a renewal assessment of a cloud service shall cover all parts of the assessment methods defined in Annex B: (Meta-approach for the assessment of cloud services), Annex C: (Assessment for levels Substantial and High), Annex D: (Assessment for level Basic) for all EUCS requirements defined in Annex A: (Security Objectives and requirements for Cloud Services).

However, in the context of a renewal assessment, some controls may not have changed since the last assessment. In such cases, the CAB may consider the previous assessment they have made of the suitability of the design in their analysis, provided that they put their focus on the changes in the risk environment and the potential impact of these changes on the controls.

G.1.3 Restoration assessment

In the restoration assessment, the objective is to perform a highly focused conformity assessment on the measures taken by the CSP to fulfil some EUCS requirements for which major nonconformities have been detected.

In a restoration assessment, the conformity assessment shall include at least the following activities.

Analysis of the change in the cloud service

These activities are required at all assurance levels.

The CAB shall at least:

- Obtain an understanding of the changes operated since the last assessment in the cloud service and the CSP's controls to meet the Security Objectives and related Security Requirements;
- Determine a list of affected controls, based on the CSP's Impact Assessment and if needed on additional inquiries;
- Assess the suitability of the design of the modified controls;
- Assess the existence and implementation of the modified controls;
- Determine whether the changes on the controls are sufficient to fulfil all the EUCS requirements for which major nonconformities have been detected

Effectiveness assessment

These activities are only required at assurance levels Substantial and High.

The CAB shall at least:

- Assess the operating effectiveness of modified controls over the period since the previous assessment of operating effectiveness.

Since the controls have been affected by the changes in the cloud service since their last assessment and if they have been operating for less than 3 months (6 months for level High), the CAB shall assess to which extent of the changes affect their ability to assess the operating effectiveness of the controls.

G.1.4 Ad hoc assessment

An ad hoc assessment can be triggered by a CSP at any time, typically after performing significant changes to their cloud service or their security controls, which require a specific assessment.

The mandatory activities for an ad hoc assessment are therefore the same as for a periodic assessment.

G.2 RE-ASSESSMENT AND AUDITS FOR COMPLIANCE MONITORING

Specific procedures may be triggered by the NCCA in the context of compliance monitoring, which are described below.

G.2.1 Re-assessment

NCCAs are required in the context of the compliance monitoring process to perform a number of re-assessments every year, depending on the number of certificates issued or maintained during the previous year.

In the first step of the re-assessment, the NCCA shall perform again the review phase performed by the CAB before taking the decision to issue or maintain the certificate, based on the documentation that was available at the time to the reviewer.

If needed for their review, the NCCA may contact the CSP in order to be granted access to the documents for which they have only provided restricted access to the CAB during the audit.

Following this review, the NCCA may request additional information about any of the activities performed during any stage of the conformity assessment. For each activity, the NCCA may:

- request additional information and explanations from the CAB;
- have the CAB perform the activity again, possibly while monitored by a NCCA representative;
- have a NCCA representative perform the activity again.

Any NCCA representative being granted access to information from the CSP or performing any conformity assessment shall be submitted to the same requirements as CAB employees performing similar activities.

The CSP shall support re-assessment activities as they supported the original conformity assessment activities.

G.2.2 Compliance audits

The NCCA may request a compliance audit if they have some reasons to doubt that a CSP complies to all their obligations with respect to the scheme, for instance after receiving a complaint.

The NCCA shall address a compliance audit request to the CAB, indicating the potential non-compliance that is suspected. Then, the process should be as follows:

- The CAB shall transmit the request to the CSP, after adding any information that they deem suitable based on their knowledge of the certified cloud service;
- The CSP shall then analyse the request and provide a motivated answer to the CAB, describing in particular any non-compliance or nonconformity they may have detected in their analysis, accompanied by supporting documentation if required;
- The CAB shall then analyse the answer from the CSP, and transmit the CSP's answer with their analysis back to the NCCA.

If the CSP does not confirm the CSP's analysis, then the NCCA shall take the final decision after consulting both parties.

If non-compliance or nonconformities have been detected, then the appropriate process(es) shall be triggered.

ANNEX H: PEER ASSESSMENT

PURPOSE	This annex describes the applicable procedure for peer assessments
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 22, Peer Assessment

Foreword for Reviewers

This Annex has been integrated recently, and it has not yet reviewed by the TG5 thematic group.

This Annex is an adaptation of the Annex 12 of the EUCC scheme. Because the topic is quite generic and covers the general organization of peer assessment rather than detailed technical requirements, the content has been only slightly modified.

Because the content has been adapted from EUCC, there may be leftover references to products, Common Criteria, ITSEFs, and other terms that normally don't belong to EUCS. Please flag such issues, and take note that there is no willingness to use these terms here.

H.1 SCOPE

This annex describes the applicable procedure for peer assessments. The procedure consists of four phases: preparation, site visit, reporting, and adoption of a report.

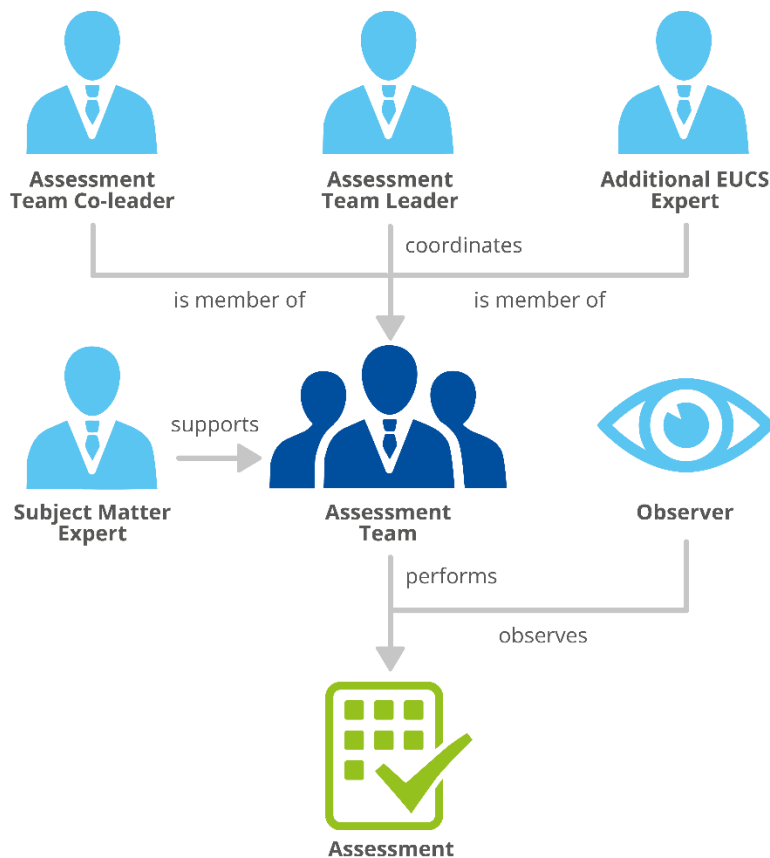
The procedure only defines the process to be followed. In order to be as comprehensive and objective as possible, checklists shall be further developed in cooperation with the ECCG to assist the peer assessment team. These checklists will contain a common understanding of state of the art²³ and operating practices.

H.2 OVERVIEW

The primary assessment team shall consist of two EUCS experts (Leader and co-Leader) selected from two CABs issuing certificates at the assurance level High of the EUCS.

This primary assessment team may be extended with additional EUCS experts from other or the same CABs, and in the case of a delegation of the issuance of certificates or of prior approval of certificates, an expert from the concerned NCCA may be associated to the selected CAB expert into the team.

Figure 6: Assessment team organisation



Each EUCS expert in the assessment team shall have a minimum of two years of experience as a certifier at a CAB issuing EUCS certificates at assurance level High. In addition, at least one EUCS expert in the assessment team shall have previously participated to the assessment of competences of CABs issuing certificates at level High, as listed in Chapter 7 (Specific requirements applicable to a CAB).

²³ As discussed in cooperation with the ECCG and/or relevant subgroups.

The peer assessment team may be assisted by subject matter experts. Those experts may be certifiers themselves, but that is not essential.

It is also highly recommended that the peer assessment team members have participated in previous peer assessments under the EUCS scheme, either as observers or team members.

The peer assessment may be observed by observers proposed by other NCCAs.

The peer assessed CAB may present to the ECCG any concern it has about the choice of the peer assessment team members and observers, for example in case of a conflict of interest

The peer assessment activities will be carried out in four phases.

The preparation phase will involve the review of the CAB documentation by the members of the peer assessment team in order to become familiar with the CAB's policies and procedures.

The site visit phase will consist of a two-week visit by the peer assessment team to the CAB in order to assess the CAB's technical competence, and where applicable of auditors performing evaluation activities. The exact duration of site visit will depend on the possible reuse of existing peer assessment evidence and results, and on the number of auditors subcontracted by the CAB.

The peer assessment will include a reporting phase: the assessment team will document their findings in a peer assessment report delivered to the ECCG.

The peer assessment will conclude with the adoption of an opinion by the ECCG of the outcome of the peer assessment.

H.3 SCHEDULING PEER ASSESSMENT ACTIVITIES

In accordance with the planning established by the ECCG, and taking into consideration the possible priorities indicated in Chapter 22, Peer Assessment, the ECCG shall notify the CAB of the peer assessment, and will task a peer assessment team to perform the peer assessment.

The peer assessed CAB shall submit the required number of candidate services for which the CAB has performed a conformity assessment, for review by the peer assessment team. In general the candidate services shall cover all technical aspects of the audit.

The required number of candidate services is:

- At least two (2) services; and
- At least one (1) service for every auditor accredited as subcontractor for the CAB at assurance level High, if applicable.

The requested information and the list of candidate products (and auditors) shall be provided by the peer assessed CAB to the peer assessment team within one month after the notification by the ECCG.

The assessment team will arrange the dates for the peer assessed CAB and where applicable auditor(s) site visit(s).

H.4 RESPONSIBILITIES OF THE PEER ASSESSED CB

The peer assessed CAB shall provide the following documentation:

- a full description of its scope, organization and operation, including:
 - the title, address and principal point of contact;
 - its role according to Article 56;
 - the accreditation decision for the CAB;

- the procedures for certification;
- where applicable, the procedures for the prior approval for each individual certificate or the requirements from a general delegation;
- the rules applying within the peer assessed CB and its internal or external auditors to the protection of protected other sensitive information;
- the titles and addresses of the auditors participating in the activities and their status (commercial or governmental);
- the procedures by which the peer assessed CAB ensures that auditors apply the evaluation criteria and methods correctly and consistently and protect the confidentiality of sensitive information involved;
- the latest list of the certificates issues by the peer assessed CAB for the last five years;
- two or more certificates and Certification Reports issued which are selected by the peer assessment team;
- where reuse of the results of a previous peer assessment is proposed, associated results, under the conditions of Chapter 22, Peer Assessment;
- the list of all auditors that perform evaluations for that domain and a description of the evidence used when assessing the competences of these auditors.

In addition, all relevant information about the quality management system that has been implemented by the CAB in order to obtain accreditation by its NAB shall be provided. It should be noted that this information is provided for informative purposes and that the content of this information is not the focus of the peer assessment. Any deviations from processes described in these documents that are found shall however be reported.

All written documentation and communications for the peer assessment activities must be provided in English at least 4 weeks before the audit date.

During the site visit, English will be spoken, unless the CAB and the peer assessment team unanimously agree upon another language.

One part of the peer assessment activities during the site visit will involve a review of at least one evaluation that has been completed or is close to being completed within the CAB.

Although the conformity assessments for chosen services submitted for consideration need not be entirely complete, there must be records showing that significant evaluation analysis and certification activities have been performed, and that the majority of the evaluation report has been delivered to and reviewed by the certification team.

In addition to the selected services, the CAB may also provide the peer assessment team with information on (up to) another two conformity assessments which were completed in the 12 months prior to the start of the peer assessment activities. If the peer assessment team has sufficient time and resources, they will review these conformity assessments during their site visit and, if they are found to be compliant with the EUCS scheme requirements, will take them into consideration within the peer assessment report.

The CAB is responsible for preparing, documenting and providing general information on the candidate services. This information will be provided to the peer assessment team for their review and selection and shall include:

- a brief overview of the product,
- the status of the conformity assessment (if not completed, then indicate what parts have been completed and what remains to be done),
- the target assurance level,
- any Security Profile compliance claims.

The peer assessment team will select at least one candidate evaluation(s) to be assessed during the site visit(s) of the CAB and where applicable of the auditor(s).

The CAB will identify a Point of Contact who will be the individual responsible for facilitating the peer assessment activities and for interacting with the assessment team leader.

The CAB Point of Contact is responsible for:

- Coordinating the site visit(s) dates and location(s) with the peer assessment team,
- Delivering the CAB materials to the peer assessment team during the Preparation Phase at least 4 weeks before the audit date,
- Coordinating any required auditor(s) visits with the peer assessment team,
- Arranging all necessary approvals to allow the peer assessment team to perform the CB and auditor(s) site visits and to have access to all information required to complete the peer assessment activities,
- Coordinating the peer assessment agenda for the CAB, including scheduling certifiers for peer assessment team interviews and briefings, ensuring the availability of materials to be reviewed during the site visit, etc.,
- Providing the peer assessment team with the ability to have copies and printouts made for use during the site visit;
- Providing secure storage, if required, for the peer assessment team's documents (e.g. lunchtime, overnight);
- Being generally available to answer questions and resolve issues that may arise during the site visit,
- Coordinating the review of the peer assessment report by CAB representatives,
- Providing feedback to the peer assessment team leader on the peer assessment draft report.

The CAB must have private room(s) available that is (are) large enough to accommodate the peer assessment team and CAB personnel during the site visit(s). Such room(s) will serve as the meeting room throughout the site visit. Accessibility to records and CAB personnel will be needed throughout the site visit in the meeting room.

H.5 RESPONSIBILITIES OF THE PEER ASSESSMENT TEAM LEADER

One member of the peer assessment team will be designated the team leader. The team leader is responsible for the following tasks:

- Coordinating the receipt of materials from the CAB,
- Coordinating the decision regarding the selection of the candidate services (and auditors) and notification to the peer assessed CAB,
- Drafting the site visit(s) agenda and coordinating it with the CB,
- Coordinating and completing the peer assessment draft report at the end of the site visit,
- Delivering the peer assessment final report to the ECCG, and
- If necessary, monitoring the CAB's resolution of outstanding issues resulting from the peer assessment.

H.6 PREPARATION PHASE

The peer assessment team should begin preparation approximately four weeks before the site visit. The peer assessed CAB shall provide the peer assessment team with access to all written policies and operating procedure documents four weeks before the site visit. Electronic and/or hardcopy documentation have to be provided, depending on the preference of the peer assessment team members and nature of documentation needed. The peer assessment team should focus their review of the documentation on gaining an understanding of the CAB's standard operating procedures.

The peer assessment team leader will coordinate the review of materials during the preparation phase. If there is a large amount of material to be reviewed, the team may divide it so that members review different portions of the documentation. The team leader will also draft and finalize the site visit(s) agenda, with input from the team members, at the conclusion of the preparation phase. The site visit(s) agenda must be forwarded to the peer assessed CAB no later than one week before the site visit(s). It is recommended that the peer assessment team leader should maintain close contact with the CAB Point of Contact during the preparation phase to keep the CAB informed of areas that will require further investigation during the site visit.

Previous peer assessment results with associated results may be proposed by the CAB for consideration by the peer assessment team.

H.7 SITE VISIT PHASE

H.7.1 Determine that the constitution and procedures of the CB comply with the general requirements of the EUCC scheme

A checklist shall be used to determine if the processes that the CAB uses to provide its conformity assessment services are sufficient to ensure effective oversight of evaluations and to ensure that successful certifications comply with the requirements of the EUCS scheme.

The CAB shall provide any relevant information associated to its accreditation to support this determination.

Where the peer assessment team decides to check some procedures of the CAB, this should occur before the assessment process commences. Nevertheless, the peer assessment team should check that the CAB is applying its procedures. This can be done at the site visit (see below) for the particular conformity assessments being assessed.

H.7.2 Perform the peer assessment

The peer assessment team should allocate two (2) full weeks for the site visit(s). If the peer assessment is completed in a shorter period of time, the team will not need to stay the full two weeks.

The peer assessment team shall have access to all evaluation and certification documentation that was used by the CAB during its conformity assessment process and especially when reviewing the evaluation documentation, and shall be permitted to observe all activities carried out during such review. If an evaluation team/certifier meeting occurs during the site visit, the peer assessment team should observe the meeting.

The peer assessment team should not completely review the work of the auditor, which may be covered by its own accreditation. However, the peer assessment team should assess whether the deliverables available to the CAB are of sufficient quality to allow the CAB to determine that the evaluation was conducted in accordance with the appropriate methodology.

The peer assessment team will make a determination of an auditor's technical competence by:

- a visit of the auditor's site,
- interviews with audit team members on technical items related to the assessment of EUCS requirements.

Findings corresponds either to

- nonconformities that are linked to a requirement from the applicable checklist or to common understanding of state of the art and operative practices that are not met (or not fulfilled). The latter will be discussed with the ECCG and could, where appropriate, be incorporated as a new item into the lists for use by future peer assessments.
- or observations that correspond to improvement proposals made by the peer assessment team, not directly linked to requirements from the checklist.

A non-conformity could be either critical or non-critical. A critical non-conformity challenges the reliability of the results established by the assessed CAB. The peer assessment team shall analyse and describe the impact of each critical non-conformity.

At the end of the site visit, the peer assessment team should present the list of findings (at least the draft list of non-conformities associated to their criticality level) to the peer assessed CAB, so that the assessed CAB can establish a proposed action plan to cover the findings. The peer assessment team should provide the final list of nonconformities (associated to their criticality level) not later than 4 weeks after the site visit to the peer assessed CAB.

If non-conformities have been identified, the CAB may request the support of the peer assessment team for establishing an action plan associated to a timescale to implement the relevant measures.

H.8 REPORTING

The peer assessment team shall produce a report that summarizes and explains their findings.

The report should be agreed internally within the peer assessment team. If the peer assessment team cannot agree internally, then majority and minority opinions shall be included in the report.

The CAB's disagreement on findings can be incorporated to the report, no later than one month after the report has been established.

The report shall also present the position of the peer assessment team on the relevance of proposed action plan to cover the findings, if this plan was submitted to the team prior to the delivery of the report to the ECCG. If evidence that cover critical non conformity is provided before issuance of the report, the team can reconsider the criticality of the non-conformity and shall document this change in the report.

The assessment team might include into its report relevant outcomes and findings from other peer assessments reused.

Findings from the peer assessment team included in the report shall be clearly identified, with a unique and unambiguous identifier.

The final report shall be produced within three months after the site visit and will be reviewed by the peer assessed CAB prior to distribution to the ECCG.

For preparation of the final report the following steps will be followed:

1. the peer assessment team will prepare a draft report, including all findings, unresolved minor and major non-conformities detected during the peer assessment in the preparation phase and the site visit phase, and deliver it for comments to the assessed CAB (one month);
2. the assessed CAB will comment the draft report, highlighting any points of disagreement and proposing changes to the report (one month);
3. the peer assessment team will consider the comments received by the CB and produce a final report with possible revisions (one month).

All three documents at points 1-3 will be delivered to the ECCG by the peer assessment team to give evidence of the final reporting phase of the peer assessment.

If any deviations of relevance for the NAB have been found, the NAB shall be informed.

The report shall provide one of three possible verdicts:

Pass: The CAB has met all requirements and no measure is required.

Pass with controlled (minor) nonconformities: The CAB has not met all requirements, but has provided a relevant actions plan and an acceptable timescale for correcting the nonconformities identified by the peer assessment team. There is no remaining critical nonconformity identified in the report.

Fail: The CAB has not met the requirements and has not provided a relevant action plan and an acceptable timescale for correcting the nonconformities identified by the peer assessment team

The peer assessment team leader (or a suitable representative with full knowledge of the assessment) shall present the report to the ECCG, including any disagreement within the team of with the peer assessed CAB. He/she shall present the findings of the team and its appreciation of how the measures proposed by the CAB will solve the issues.

Where relevant, appropriate additions will be made to the assessment checklist to assist future peer assessment teams.

H.9 ADOPTION OF PEER ASSESSMENT REPORT

The following procedure is provided to guarantee adequate involvement of the assessed CB to demonstrate prompt resolution of non-conformities. The procedure also helps limiting the time for the adoption of the peer assessment.

1. The ECCG will request the ECCG subgroup dedicated to maintenance of the EUCS scheme to prepare an opinion to be adopted by the ECCG on the conducted peer assessment.
2. The ECCG subgroup will meet to discuss the result of the peer assessment (based on documents 1-3) and invite for the meeting the peer assessment team and the assessed CAB. Following the meeting, one of the following proposals of opinion will be issued by the ECCG subgroup:
 - the final report from the assessment team is proposed to be adopted as it is;
 - an amended final report from the assessment team is proposed to be adopted.

In the case of non-conformities, the opinion to be adopted by the ECCG will include a recommendation to the assessed CAB to resolve such non-conformities with an indication of the duration allocated to this resolution. This duration should be limited to 2 months in the general case and should not exceed 6 months.

3. the ECCG subgroup will deliver to the ECCG:

- the minutes of the meeting;
- the proposed opinion to be adopted by the ECCG.

The ECCG subgroup shall ensure that any feedback on non-conformities or recommendations received by the CAB that underwent the peer assessment or the NAB will be forwarded along to the ECCG.

4. The ECCG will provide its opinion on the draft opinion. In the case of favourable opinion, the assessed CAB will:

- either pass the peer assessment (if the draft opinion indicated a positive verdict of the peer assessment). The positive verdict will be published on ENISA website directly with the accompanying peer assessment findings.
- or be recommended to take the necessary actions to resolve the non-conformities in the allocated duration. The recommendation will not be published on the ENISA website.

The ECCG may also request the ECCG subgroup to re-examine the peer assessment (starting at point 2. again), only one time.

5. When corrective actions are requested by the ECCG to the CAB, following the implementation of the corrective actions, the assessed CAB will issue a report to the ECCG subgroup within 2 months

6. The ECCG subgroup will hold a meeting within 2 months with the assessed CAB and the assessment team to discuss the status of resolution of the non-conformities. The lack of a report from the assessed CAB will not prevent the ECCG subgroup to have the meeting.

7. The ECCG subgroup will prepare an opinion to be adopted by the ECCG containing either a pass (successful correction of non-conformities) or a fail (residual non conformities already in place) and will deliver the proposed opinion and the minutes of the meeting to the ECCG.

8. The ECCG will establish its opinion based on the draft opinion and adopt the final result (including residual recommendation, or no recommendation for the CAB). The ECCG will adopt the proposed opinion or adopt its own opinion, without recurring to further iterations with the ECCG subgroup. The opinion adopted by the ECCG will be published with all relevant documents on the ENISA website.

ANNEX I: TERMINOLOGY

PURPOSE	This annex describes the applicable terminology for the candidate scheme
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	All chapters and annexes

Foreword for Reviewers

This Annex defines some vocabulary to be used in the draft candidate scheme.

Its first section defines certification-related terminology. It mostly draws from [ISO17000] and related standards, and also from other standards such as ISAE standards. This first section will later be reduced in order to leave only the terms that are actually used in the draft candidate scheme, but the full content is left for now as a reference.

Its second section defines more general vocabulary, which is used in particular in Annex A: (Security Objectives and requirements for Cloud Services). Please refer to that section in case of doubt regarding a term used in that annex. The section is less mature and some definitions will need to be revised.

.



I.1 CERTIFICATION TERMINOLOGY

The following terminology mostly comes from ISO standards (ISO17000, ISO17021, ISO17025, ISO17065) and EU regulations.

WARNING! This is work in progress, so the definitions will evolve over time.

I.1.1 Components

Term	Definition
requirement	<p>need or expectation that is stated, generally implied or obligatory</p> <p>Note 1 to entry: “Generally implied” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.</p> <p>Note 2 to entry: A specified requirement is one that is stated, for example in documented information.</p> <p>Note 3 to entry: A qualifier can be used to denote a specific type of requirement, e.g. product requirement, service requirement, customer requirement.</p> <p>[SOURCE: From ISO27000:3.56]</p>
specified requirement	<p>need or expectation that is stated</p> <p>Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications.</p> <p>Note 2 to entry: Specified requirements can be detailed or general</p> <p>Note 3 to entry: In the context of a European cybersecurity certification scheme, the specified requirements typically correspond to the requirements specified in the scheme, either directly or indirectly (in normative documents referred to in the scheme).</p> <p>[SOURCE: From ISO17000(2020):5.1]</p>
product requirement	<p>requirement that relates directly to a product, specified in standards or in other normative documents identified by the certification scheme</p> <p>Note 1 to entry: Product requirements can be specified in normative documents such as regulations, standards and technical specifications.</p> <p>[SOURCE: From ISO17065:3.8]</p>
operational requirement	<p>requirement that relates directly to the operation of a service, specified in standards or in other normative documents identified by the certification scheme</p> <p>[SOURCE: Inspired from ISO17065:3.8]</p>
audit criteria	<p>set of requirements used as a reference against which objective evidence is compared</p> <p>Note 1 to entry: Requirements may include policies, procedures, work instructions, legal requirements, contractual obligations, etc.</p> <p>[SOURCE: ISO19011:3.7]</p>
claim	<p>information declared by the client</p> <p>Note 1 to entry: The claim is the object of conformity assessment by validation or verification.</p> <p>Note 2 to entry: The claim can represent a situation at a point in time or could cover a period of time.</p> <p>Note 3 to entry: The claim should be clearly identifiable and capable of consistent evaluation or measurement against specified requirements by a conformity assessment body.</p> <p>Note 4 to entry: The claim can be provided in the form of a report, a statement, a declaration, a project plan, or consolidated data.</p> <p>Note 5 to entry: We may need to change this definition in order to give it a more general meaning.</p> <p>[SOURCE: From ISO17029:3.1]</p>

Term	Definition
objective	<p>result to be achieved</p> <p>Note 1 to entry: An objective can be strategic, tactical, or operational.</p> <p>Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and process].</p> <p>Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target).</p> <p>Note 4 to entry: In the context of information security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.</p> <p>[SOURCE: From ISO27000:3.49]</p>
objective evidence	<p>data supporting the existence or verity of something</p> <p>Note 1 to entry: Objective evidence can be obtained through observation, measurement, test, or by other means.</p> <p>Note 2 to entry: Objective evidence for the purpose of audit generally consists of records, statements of fact or other information which are relevant to the audit criteria and verifiable.</p> <p>[SOURCE: From ISO9000:3.8.3]</p>
sufficiency of evidence	<p>The measure of the quantity of evidence</p> <p>[SOURCE: From ISAE3000: 12.i.i]</p>
appropriateness of evidence	<p>The measure of the quality of evidence</p> <p>[SOURCE: From ISAE3000: 12.i.ii]</p>
characteristic	<p>distinguishing feature</p> <p>Note 1 to entry: A characteristic can be inherent or assigned.</p> <p>Note 2 to entry: A characteristic can be qualitative or quantitative.</p> <p>[SOURCE: From ISO9000:3.10.1]</p>
component	<p>an entity with discrete structure within a system considered at a given level of analysis</p> <p>[SOURCE: Wikipedia]</p>
system	<p>a group of interacting or interrelated entities that form a unified whole</p> <p>[SOURCE: Wikipedia]</p>
subsystem	<p>a set of elements, which is a system itself, and a component of a larger system</p> <p>[SOURCE: Wikipedia]</p>
management system	<p>set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives</p> <p>Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.</p> <p>Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.</p> <p>Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.</p> <p>[SOURCE: ISO9000:3.5.3]</p>
procedure	<p>specified way to carry out an activity or a process</p> <p>Note 1 to entry: Procedures can be documented or not.</p> <p>[SOURCE: ISO 9000:2000, 3.4.5]</p>
policy	<p>intentions and direction of an organization, as formally expressed by its top management</p>

Term	Definition
	[SOURCE: ISO Supplement, 3.7]
product	output of an organization that can be produced without any transaction taking place between the organization and the customer [SOURCE: ISO 9000:2000, 3.4.2]
ICT product	an element or a group of elements of a network or information system Note 1 to entry: In the definition of certification schemes, the use of 'ICT product' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. It is a subset of the more general term product, whose definition originates in ISO9000. [SOURCE: From EC881/2019:2.12]
output	result of a process Note 1 to entry: Whether an output of the organization is a product or a service depends on the preponderance of the characteristics involved, e.g. a painting for sale in a gallery is a product whereas supply of a commissioned painting is a service, a hamburger bought in a retail store is a product whereas receiving an order and serving a hamburger ordered in a restaurant is part of a service. [SOURCE: From ISO9000:5.6]
process	set of interrelated or interacting activities which transforms inputs into outputs [SOURCE: From ISO Supplement:3.12]
ICT process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service Note 1 to entry: This term is to be used when a process is intended to be the object of a cybersecurity certification. The term 'process' is more general and should be used in other situations. [SOURCE: From EC881/2019:2.14]
service	output of an organization with at least one activity necessarily performed between the organization and the customer Note 1 to entry: This definition from ISO9000 echoes the definition of a product, and is refined into the notion of information service from European Regulation 1535/2015. [SOURCE: From ISO 9000:2000, 3.7.7]
information service	any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Note 1 to entry: For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request. [SOURCE: From EC1535/2015:1.b]
ICT service	a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems Note 1 to entry: In the definition of certification schemes, the use of 'ICT service' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and products certified using such schemes. For a more general use, it is preferable to use the term 'service'. [SOURCE: From EC881/2019:2.13]
composed service composite service	service comprised of two or more components that have been successfully certified [SOURCE: Inspired from ISO15408, 3.6.4]

Term	Definition
base service	entity in a composed service, which has itself been the subject of a conformity assessment, providing services and resources to a dependent service [SOURCE: Inspired from ISO15408, 3.6.1]
dependent service	entity in a composed service, which is itself the subject of a conformity assessment, relying on the provision of services by a base services [SOURCE: Inspired from ISO15408, 3.6.5]
object of conformity assessment object	entity to which specified requirements (5.1) apply EXAMPLE: Product, process, service, system, installation, project, data, design, material, claim, person, body or organization, or any combination thereof. [SOURCE: From ISO17000(2020):4.2, Note 2]
assurance level	a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned Note 1 to entry: A scheme often defines discrete assurance levels, and each such discrete level defines a degree of confidence in the fulfilment of requirements by the ICT product, ICT service, or ICT process. [SOURCE: From EC 881/2019, 2.21]
conformity	fulfilment of a requirement Note 1 to entry: when used in opposition with compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO Supplement:3.18]
compliance	conformity in the context of a the rules and requirements defined in a certification scheme. Note 1 to entry: This is a refinement of ISO19011, which defines compliance as conformity in the context of a statutory requirement or regulatory requirement. In this case, compliance is conformity in the context of a given scheme. [SOURCE: Inspired from ISO19011:3.7]
nonconformity	non-fulfilment of a requirement Note 1 to entry: when used in opposition with non-compliance, conformity relates to the requirements related to the object of conformity assessment rather than to the requirements related to the certification scheme. [SOURCE: From ISO Supplement:3.19]
major nonconformity	nonconformity that affects the capability of the management system to achieve its intended results Note 1 to entry: Nonconformities could be classified as major in the following circumstances: <ul style="list-style-type: none"> - if there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements; - a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity. [SOURCE: Adapted from ISO17021:3.12]
minor nonconformity	nonconformity that does not affect the capability of the management system to achieve its intended results
non-compliance	nonconformity in the context of the rules and requirements defined in a certification scheme Note 1 to entry: This is a refinement of ISO19011, which defines non-compliance as nonconformity in the context of a statutory requirement or regulatory requirement. Here, compliance is conformity in the context of a given scheme. [SOURCE: Inspired from ISO19011:3.7]

Term	Definition
control	<p>measure that is modifying risk</p> <p>Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.</p> <p>Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.</p> <p>[SOURCE: ISO Guide 73:3.8.11]</p>
control objective	<p>statement describing what is to be achieved as a result of implementing controls</p> <p>[SOURCE: ISO27000:3.15]</p>
compensating control	<p>An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions</p> <p>[SOURCE: SOC2]</p>
detective control	<p>A control that detects and reports when errors, omissions and unauthorized uses or entries occur</p> <p>[SOURCE: SOC2]</p>
preventive control	<p>An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product</p> <p>[SOURCE: SOC2]</p>
effectiveness	<p>extent to which planned activities are realized and planned results achieved</p> <p>[SOURCE: ISO Supplement:3.6]</p>
design effectiveness	<p>Refers to the suitability of the control as of a specified date or for a specified period (typically 6 to 12 months), based on the auditor's conclusion on whether</p> <ul style="list-style-type: none"> (i) the risks that threaten the achievement of the control objectives have been identified by management; (ii) the controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives from being achieved. <p>[SOURCE: Inspired from ISAE3402]</p>
operating effectiveness	<p>A control is operating effectively, if</p> <ul style="list-style-type: none"> (i) it was consistently applied as designed throughout the specified period, and (ii) in case of manual controls, they were applied by individuals who have the appropriate competence and authority. <p>[SOURCE: Inspired from ISAE3402]</p>
asset	<p>item, thing or entity that has potential or actual value to an organization</p> <p>Note 1 to entry: Value can be tangible or intangible, financial or non-financial, and includes consideration of risks and liabilities. It can be positive or negative at different stages of the asset life.</p> <p>Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation or agreements.</p> <p>Note 3 to entry: A grouping of assets referred to as an asset system could also be considered as an asset.</p> <p>[SOURCE: From ISO55000]</p>
asset life	<p>period from asset creation to asset end-of-life</p> <p>[SOURCE: From ISO55000]</p>
life cycle	<p>stages involved in the management of an asset</p> <p>Note 1 to entry: The naming and number of the stages and the activities under each stage usually vary in different industry sectors and are determined by the organization.</p> <p>[SOURCE: From ISO55000]</p>

Term	Definition
asset system	set of assets (3.2.1) that interact or are interrelated [SOURCE: From ISO55000]
risk	effect of uncertainty on objectives Note 1 to entry: An effect is a deviation from the expected — positive and/or negative. Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. [SOURCE: From ISO Guide 73:1.1]
operational risk	A risk arising from execution of a company's business functions
engagement risk	The risk that the practitioner expresses an inappropriate conclusion when the subject matter information is materially misstated [SOURCE: From ISAE3000: 12.f]
risk of material misstatement	The risk that the subject matter information is materially misstated prior to the start of the engagement [SOURCE: From ISAE3000: 12.w]
control risk	the risk that an event that prevents a security requirement from being met will not be prevented or detected and corrected on a timely basis by the controls
security event	An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems [SOURCE: TSC]
security incident	A security event that requires action on the part of an entity in order to protect information assets and resources [SOURCE: TSC]
compromise	Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs [SOURCE: TSC]
carve-out method	Method of dealing with the services provided by a subservice organization, whereby the service organization's description of its system includes the nature of the services provided by a subservice organization, but that subservice organization's relevant control objectives and related controls are excluded from the service organization's description of its system and from the scope of the service auditor's engagement. The service organization's description of its system and the scope of the service auditor's engagement include controls at the service organization to monitor the effectiveness of controls at the subservice organization, which may include the service organization's review of an assurance report on controls at the subservice organization. [SOURCE: From ISAE3402: 9.a]
inclusive method	Method of dealing with the services provided by a subservice organization, whereby the service organization's description of its system includes the nature of the services provided by a subservice organization, and that subservice organization's relevant control objectives and related controls are included in the service organization's description of its system and in the scope of the service auditor's engagement [SOURCE: From ISAE3402: 9.g]

I.1.2 Activities

Term	Definition
conformity assessment	<p>demonstration that specified requirements are fulfilled</p> <p>Note 1 to entry: The process of conformity assessment [...] can have a negative outcome, i.e. demonstrating that the specified requirements are not fulfilled.</p> <p>Note 1 to entry: The subject field of conformity assessment includes selection activities, determination activities such as testing, inspection and audit, review activities, and attestation activities such as certification, as well as the accreditation of conformity assessment bodies.</p> <p>Note 3 to entry: [ISO17000] does not include a definition of “conformity”. “Conformity” does not feature in the definition of “conformity assessment”. Nor does [ISO17000] address the concept of compliance.</p> <p>[SOURCE: From ISO17000(2020):4.1, some modifications in notes]</p>
activity	<p>smallest identified object of work in a given context</p> <p>[SOURCE: From ISO9000:3.3.11]</p>
first-party conformity assessment activity	<p>conformity assessment activity that is performed by the person or organization that provides the object of conformity assessment</p> <p>[SOURCE: From ISO17000(2020):4.3]</p>
third-party conformity assessment activity	<p>conformity assessment activity that is performed by a person or organization that is independent of the provider of the object of conformity assessment, and has no user interest in the object</p> <p>[SOURCE: From ISO17000(2020):4.5]</p>
conformity self-assessment	<p>first-party conformity assessment activities, which evaluate whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme</p> <p>Note 1 to entry: The original definition from EC 881-2019 has been reworded to make the link with the definition of a first-party conformity assessment activity, but the meaning remains unchanged.</p> <p>[SOURCE: From EC881/2019:2.22]</p>
selection	<p>planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function</p> <p>Note 1 to entry: Selection activities vary widely in number and complexity. In some instances, very little selection activity may be needed.</p> <p>[SOURCE: From ISO17000:A.2.1]</p>
sampling	<p>selection and/or collection of material or data regarding an object of conformity assessment</p> <p>Note 1 to entry: Selection can be on the basis of a procedure, an automated system, professional judgement etc.</p> <p>Note 2 to entry: Selection and collection can be performed by the same or different persons or organizations.</p> <p>[SOURCE: From ISO17000(2020):6.1]</p>
determination	<p>activities undertaken to develop complete information regarding fulfilment of the specified requirements by the object of conformity assessment or its sample</p> <p>[SOURCE: From ISO17000:A.3.1]</p>
testing	<p>determination of one or more characteristics of an object of conformity assessment, according to a procedure</p> <p>Note 1 to entry: The procedure can be intended to control variables within testing as a contribution to the accuracy or reliability of the results.</p>

Term	Definition
	<p>Note 2 to entry: The results of testing can be expressed in terms of specified units or objective comparison with agreed references.</p> <p>Note 3 to entry: The output of testing can include comments (e.g. opinions and interpretations) about the test results and fulfilment of specified requirements.</p> <p>[SOURCE: From ISO17000(2020):6.2]</p>
inspection	<p>examination of an object of conformity assessment and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements</p> <p>Note 1 to entry: Examination can include direct or indirect observations, which can include measurements or the output of instruments.</p> <p>Note 2 to entry: Conformity assessment schemes or contracts can specify inspection as examination only.</p> <p>[SOURCE: From ISO17000(2020):6.3]</p>
audit	<p>process for obtaining relevant information about an object of conformity assessment (4.2) and evaluating it objectively to determine the extent to which specified requirements (5.1) are fulfilled</p> <p>Note 1 to entry: The specified requirements are defined prior to performing an audit so that the relevant information can be obtained.</p> <p>Note 2 to entry: Examples of objects for an audit are management systems, processes, products and services.</p> <p>[SOURCE: From ISO17000(2020):6.4]</p>
validation	<p>confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements (5.1) have been fulfilled</p> <p>Note 1 to entry: Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use.</p> <p>[SOURCE: From ISO17000(2020):6.5]</p>
verification	<p>confirmation of truthfulness through the provision of objective evidence that specified requirements (5.1) have been fulfilled</p> <p>Note 1 to entry: Verification can be applied to claims to confirm the information declared with the claim regarding events that have already occurred or results that have already been obtained.</p> <p>[SOURCE: From ISO17000(2020):6.6]</p>
evaluation	<p>combination of the selection and determination functions of conformity assessment activities</p> <p>[SOURCE: From ISO17065:3.3]</p>
review	<p>consideration of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements by an object of conformity assessment</p> <p>[SOURCE: From ISO17000(2020):7.1]</p>
decision	<p>conclusion, based on the results of review (7.1), that fulfilment of specified requirements (5.1) has or has not been demonstrated</p> <p>[SOURCE: From ISO17000(2020):7.2]</p>
peer assessment	<p>assessment of a body against specified requirements by representatives of other bodies in, or candidates for, an agreement group</p> <p>Note 1 to entry: This entry is not satisfactory for several reasons, and in particular because it refers to concepts that are not currently defined (agreement group) and have little interest for us, and also mentions of a "body", which is unclear.</p> <p>Note 2 to entry: On the other hand, this could cover both CABs at level 'high' and NCCAs, but some rewriting is required.</p> <p>[SOURCE: From ISO17000:4.5]</p>
attestation	<p>issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated</p>

Term	Definition
	<p>Note 1 to entry: The resulting statement [...] is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees.</p> <p>Note 2 to entry: First-party attestation and third-party attestation are distinguished by the terms declaration, certification, and accreditation, but there is no corresponding term applicable to second-party attestation.</p> <p>[SOURCE: From ISO17000:5.2]</p>
scope of attestation	<p>identification of</p> <ul style="list-style-type: none"> — the product(s), process(es) or service(s) for which the attestation is granted, — the applicable conformity assessment scheme, and — the standard(s) and other normative document(s), including their date of publication, to which it is judged that the product(s), process(es) or service(s) comply <p>Note 1 to entry: The notion of scope can be similarly applied to specific kinds of attestation, such as scope of certification or scope of declaration.</p> <p>[SOURCE: From ISO17065:3.10]</p>
declaration	<p>first-party attestation</p> <p>[SOURCE: From ISO17000(2020):7.5]</p>
EU statement of conformity	<p>declaration produced by a vendor of ICT product, ICT process, or ICT service after performing a conformity self-assessment in the context of an European cybersecurity certification scheme, that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme</p>
certification	<p>third-party attestation related to an object of conformity assessment, with the exception of accreditation</p> <p>[SOURCE: From ISO17000:7.6]</p>
accreditation	<p>third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities</p> <p>[SOURCE: From ISO17000(2020):7.7]</p>
surveillance	<p>systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity</p> <p>Note 1 to entry: We may not want to keep this term, because of possible confusion with market surveillance, but it is kept for now, as some term needs to cover that concept.</p> <p>[SOURCE: From ISO17000(2020):8.1]</p>
suspension	<p>temporary restriction of the statement of conformity by the body that issued the statement, for all or part of the specified scope of attestation</p> <p>[SOURCE: From ISO17000(2020):8.2]</p>
withdrawal cancellation	<p>revocation of the statement of conformity by the body that issued the statement</p> <p>[SOURCE: From ISO17000(2020):8.3]</p>
expiry	<p>ending of the validity of the statement of conformity after a specified period</p> <p>[SOURCE: From ISO17000(2020):8.4]</p>
restoration	<p>reinstatement of the full or partial statement of conformity</p> <p>[SOURCE: From ISO17000(2020):8.5]</p>

I.1.3 Entities and roles

Term	Definition
conformity assessment body	body that performs conformity assessment services [SOURCE: From ISO17000:2.5]
accreditation body	conformity assessment body that performs accreditation Note 1 to entry: The authority of an accreditation body is generally derived from government. [SOURCE: From ISO17000:2.6]
national accreditation body	the sole body in a Member State that performs accreditation with authority derived from the State [SOURCE: From EC765/2008:2.1]
certification body	third-party conformity assessment body that performs review and certification activities.
audit team	one or more persons conducting an audit, supported if needed by technical experts Note 1 to entry: One auditor of the audit team is appointed as the audit team leader. [SOURCE: ISO9000:3.13.14]
auditor	person who conducts an audit Note 1 to entry: In the schemes and related documents, 'the auditor' is typically used as the subject of requirements related to audit of the form "the auditor shall...". [SOURCE: From ISO17021:3.6]
technical expert	person who provides specific knowledge or expertise to the audit team [SOURCE: From ISO17021:3.14]
conformity assessment system	rules, procedures and management for carrying out conformity assessment Note 1 to entry: The Cybersecurity Act is a conformity assessment system from which are derived European cybersecurity certification schemes. [SOURCE: From ISO17000:2.7]
conformity assessment scheme	conformity assessment system related to specified objects of conformity assessment, to which the same specified requirements, specific rules and procedures apply [SOURCE: From ISO17000:2.8]
certification scheme	conformity assessment scheme that includes a certification activity Note 1 to entry: In a certification scheme, a successful assessment leads to the issuance of a certificate.
European cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From EC 881/2019:2.9]
national cybersecurity certification scheme	a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme Note 1 to entry: This definition is a refinement of the definition of a certification scheme. [SOURCE: From EC 881/2019:2.10]
organization	person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private. [SOURCE: ISO Supplement:3.1]

Term	Definition
top management	<p>person or group of people who directs and controls an organization at the highest level</p> <p>Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.</p> <p>Note 2 to entry: If the scope of the management system covers only part of an organization, then top management refers to those who direct and control that part of the organization.</p> <p>[SOURCE: ISO Supplement:3.5]</p>
first-party	<p>the person or organization that provides the object of conformity assessment</p> <p>[SOURCE: From ISO17000:2.2]</p>
third-party	<p>a person or body that is independent of the person or organization that provides the object of conformity assessment, and of user interests in that object</p> <p>[SOURCE: From ISO17000:2.2]</p>
interested party stakeholder	<p>person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity</p> <p>[SOURCE: ISO Supplement:3.2]</p>

I.2 TERMS TO BE ADDED OR CONSIDERED

Foreword for Reviewers

This section is work in progress about terminology, in particular regarding the terminology used in the Security Controls, often derived from C5. The definition need to be confirmed and integrated in the main terminology.

Term	Abbreviation	Definition
Mutual Recognition Agreement	MRA	
records system		<p>information system which captures, manages and provides access (3.1) to records over time</p> <p>Note 1 to entry: A records system can consist of technical elements such as software, which may be designed specifically for managing records or for some other business purpose, and non-technical elements including policy, procedures, people and other agents, and assigned responsibilities.</p> <p>[SOURCE: From ISO15489-1:2016]</p>
Supplementary cybersecurity information		From the Cybersecurity Act

Term	Abbreviation	Definition
document		<policies and procedures> the actions of designing policies and procedures related to a given topic or process and of preparing documentation targeting the relevant stakeholders
implement establish?		<policies and procedures> the action of putting the policies and procedures into practice NOTE: C5 does not explicitly refer to implementation.
communicate		<any document or information> the action of sharing the document or information with targeted persons through an explicit action (email, posters, etc.)
make available provide?		<any document or information> the action of sharing the document or information by storing or displaying it in a place previously agreed with the targeted persons
approve		<any document or information> the action by an authorized body to confirm that a document conforms to requirements or expectations
review		<any document> the action of checking that a document is up-to-date, and unless otherwise specified, of modifying the document with up-to-date information
update		<any document> the action of modifying the document with up-to-date information
maintain		<any document> the continuous action of keeping a document up-to-date
control security control		Process-integrated or process-independent measure to reduce the likelihood of events occurring or to detect events that have occurred in order to maintain the information security of the cloud service [Source: C5:2020]
system component		the objects required for the information security of the cloud service during the creation, processing, storage, transmission, deletion or destruction of information in the Cloud Service Provider's area of responsibility EXAMPLES: firewalls, load balancers, web servers, application servers, database servers [Source: C5:2020]
authorized body		person or group of persons to whom top management has delegated a task or responsibility Note 1 to entry: In the security controls, authorized bodies would typically be responsible for of a given policy and related procedures
internal employee		employee of the CSP
external employee		employee of a third-party who is working for the CSP and who is considered as an employee in the human resource managements controls described in the HR category.
perimeter security perimeter		the physical border surrounding locations hosting CSP equipment and personnel, for which access is controlled
area security area		an area delimited by security perimeters, within which access is not controlled
datacentre		location hosting the equipment from which the cloud operates
personal account		a personal account associated to a single human user
shared account		a generic account, typically shared between several human users

Term	Abbreviation	Definition
technical account		an account associated to a non-human user, who could be an application or a device
access right		permission for a subject to access a particular asset for a specific type of operation [Source: ISO/IEC 2382:2015, 2126298]
development environment		The environment in which changes to software are developed, typically an individual developer's workstation
test environment		The environment in which new and changed code is exercised via automated or non-automated techniques
pre-production environment		Mirror of production environment used for final testing or
production environment		The environment that serves customers
service provider external service provider		organization or an individual that enters into agreement with the CSP for the supply of a service [SOURCE: Freely adapted from ISO/IEC 27036:1-2014, 3.9]
subservice provider subservice organization		third-party providing services to the CSP that contribute to the provision of the cloud service by the CSP
supplier		organization or an individual that enters into agreement with the acquirer for the supply of a product or service Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller, or vendor. Note 2 to entry: the term "service provider" is typically used in this scheme for suppliers of services Note 3 to entry: when opposed to "service provider", the term "supplier" refers to a supplier of products [SOURCE: Adapted from ISO/IEC 27036:1-2014, 3.9]



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA

European Union Agency for Cybersecurity

Athens Office

1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu



ISBN 000-00-0000-000-0