



EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme
for cloud services

V1.0.319 | MAY 2023

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Details
06/01/2020	0.1.001	Created	
13/03/2020	0.2.011	Update after kick-off	Integration of results of the discussions during the kick-off meetings, plus additional questions
17/03/2020	0.3.012	Continuing the update	
23/03/2020	0.4.013	Update after TG0 kick-off	Including a full set of questions to be answered in the context of TG0
11/05/2020	0.5.020	Update after plenary	Now including most answers to TG0 questions
25/05/2020	0.5.022	Final update on questions	Most questions now with a final answer
23/07/2020	0.6.030	First draft scheme	First draft scheme with initial contributions and feedback from the first external review
28/09/2020	0.7.040	Update after final EUCC	Update including the chapters that took inspiration from EUCC, especially around scheme processes
30/10/2020	0.8.044	For concept review	First partial consolidation for review by the AHWG and by Member States
29/11/2020	0.9.048	Intermediary version	
11/12/2020	0.9.050	Intermediary version	
22/12/2020	0.9.052	External review version	Version released publicly for review by the ECCG and the SCCG and for public review
30/07/2021	0.9.130	Version after revision and reduction	Limited release
20/08/2021	0.9.133	Further revisions, introduction of extension profiles	Released to the AHWG for review
13/10/2021	0.9.141	Reinforcement of pen testing, introduction of specific requirements	Limited release
22/10/2021	0.9.142	Various minor updates	For review in the AHWG
02/03/2022	0.9.209	Major updates	For internal review
23/03/2022	0.9.212	Minor updates after internal review	For MT review
31/03/2022	0.9.213	Minor updates after internal review	For further review
08/04/2022	1.0.214	Minor updates	For review by the Commission
20/05/2022	1.0.220	Minor updates	For review by the AHWG
28/07/2022	1.0.230	Minor updates	After review by AHWG members
16/09/2022	1.0.237	Updates on levels and more	After review by the Commission
21/10/2022	1.0.242	Updates on requirements and more	Minor updates, including a synchronisation with ongoing discussions in CEN-CENELEC JTC13 WG2 in Annex A

Date	Version	Modification	Details
15/12/2022	1.0.250	Updates on requirements and more	Minor updates, including a synchronisation with ongoing discussions in CEN-CENELEC JTC13 WG2 in Annex A
05/05/2023	1.0.319	Updates on PUA and more	

POLITICO

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 2020 to July 2022.

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(5) of the Cybersecurity Act, and shall not be used for any other purpose. After consultation, ENISA may amend it.

External 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, accessibility and accuracy 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), 2020-2023. 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 and further 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 owners or licensed holders that have the right to sub-licence.

TABLE OF CONTENTS

1. A SCHEME FOR CLOUD SERVICES	6
2. SUBJECT MATTER AND SCOPE	13
3. PURPOSE OF THE SCHEME	17
4. USE OF STANDARDS	22
5. ASSURANCE LEVELS	24
6. SELF-ASSESSMENT	36
7. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB	38
8. EVALUATION METHODS AND CRITERIA	42
9. NECESSARY INFORMATION FOR CERTIFICATION	46
10. MARKS AND LABELS	49
11. COMPLIANCE MONITORING	51
12. CERTIFICATE MANAGEMENT	56
13. NON-COMPLIANCE	61
14. NEW VULNERABILITIES	65
15. RECORD RETENTION	68
16. RELATED SCHEMES	69
17. CERTIFICATE FORMAT	71
18. AVAILABILITY OF INFORMATION	73
19. CERTIFICATE VALIDITY	74
20. DISCLOSURE POLICY	75
21. MUTUAL RECOGNITION	77
22. PEER ASSESSMENT	80

23. SUPPLEMENTARY INFORMATION	83
24. ADDITIONAL TOPICS	85
25. FURTHER RECOMMENDATIONS	89
26. REFERENCES	92
ANNEX A: SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES	95
ANNEX B: META-APPROACH FOR THE ASSESSMENT OF CLOUD SERVICES	215
ANNEX C: ASSESSMENT FOR LEVELS CS-EL2 AND ABOVE	231
ANNEX D: ASSESSMENT FOR LEVEL CS-EL1	238
ANNEX E: COMPETENCE REQUIREMENTS FOR CABS	241
ANNEX F: SCHEME DOCUMENT CONTENT REQUIREMENTS	245
ANNEX G: CERTIFICATION LIFE CYCLE AND CONTINUED ASSURANCE	278
ANNEX H: EXTENSION PROFILES	283
ANNEX I: PEER ASSESSMENT	289
ANNEX J: ANNEX J: PROTECTION OF EUROPEAN DATA AGAINST UNLAWFUL ACCESS	298
ANNEX K: TERMINOLOGY	307

1. A SCHEME FOR CLOUD SERVICES

1.1 INTRODUCTION

Following the request from the European Commission¹ in accordance with Article 48(2) of the Cybersecurity Act² (hereinafter referred to as EUCSA as indicated in the glossary), ENISA has set up an Ad Hoc Working Group (AHWG) in accordance with Article 49(4) of the EUCSA to support the preparation of a candidate EU cybersecurity certification scheme for cloud services (hereinafter referred to as EUCS as indicated in the glossary).

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 looks into the certification of the cybersecurity of cloud services. The scheme draws from many different sources, the most notable ones being the National schemes BSI C5:2020 from Germany [C5] and ANSSI SecNumCloud from France [SecNumCloud], as well as the report [CSP-CERT] of the CSP-CERT Working Group, which was delivered in 2019 and provided a basic framework on which the candidate scheme has been developed.

The EUCS supports the three assurance levels defined 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 assurance level 'high' are demanding and close to or at the state-of-the-art level, and may therefore serve to protect the most sensitive cases of cloud usage, including those related to the fundamental interest to society, or very sensitive business interests where no material compromise to cybersecurity can be expected. To serve that purpose, the EUCS also introduces a new set of requirements, related to independence of the assessed cloud service from non-EU laws, including in particular requirements about the effective control of the cloud service provider, about the location of employees and of data storage and processing. Therefore, two distinct evaluation levels have been defined for assurance level 'high', which differ on their approach to independence from non-EU laws, with level CS-EL3 focusing on technical and transparency measures, and level CS-EL4 being even more prescriptive invoking a strict approach to non-interference with data, whether personal or not, of particular sensitivity, the breach of which is likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property.

On the other end of the spectrum, the requirements at assurance 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 to ensure some security for their customers. The assurance level 'substantial', offers a reasonable level of protection, it stands in between assurance levels 'basic' and 'high' and it serves the purpose of protecting most business cases; it may be the most appropriate level for many applicants and their customers.

The candidate EUCS also defines mechanisms to support the composition of cloud services, where an application capability in a cloud service is based on another cloud service's platform or infrastructure capabilities. In such cases, if the underlying cloud service has been issued an EUCS certificate, then the audit of the application service can be simplified, by not repeating the audit of the underlying service's controls. This mechanism, however, can only be used

¹ Ares(2019)7197658 - Request for the preparation of a candidate European cybersecurity certification scheme under Article 48(2) of the Cybersecurity Act

² 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).

if the underlying service has been certified to an evaluation level at least equivalent as the one sought by the application service.

The candidate EUCS targets a specific category of ICT services, so the candidate scheme draws from the ISO/IEC 17065 standard, which is the harmonized standard for the accreditation of conformity assessment bodies (CABs) performing certification of services, as mandated by the EUCSA Annex. Regarding evaluation activities, there are two main standards suitable for the assessment of the cybersecurity of cloud services, based respectively on the ISO/IEC 17021-1 standard and on the International Auditing Standards issued by IAASB (International Auditing and Assurance Standards Board). Both approaches are commonly used to assess Information Security Management Systems, so their scope is slightly different from the scope of this candidate scheme. Nevertheless, the scheme uses an assessment approach for EUCSA assurance levels 'substantial' and 'high' that is compatible with both standards, allowing cloud service providers to easily and efficiently integrate the scheme into their current certification and assurance strategy.

The candidate EUCS also defines a simplified assessment methodology for the EUCSA assurance level 'basic'. The methodology is based on evidence provided by the cloud service provider through an internal audit, whose sufficiency and appropriateness are then audited by a conformity assessment body. However, the candidate scheme does not allow cloud service providers to issue EU statements of conformity.

Finally, the EUCS 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 leverages principles that were first defined in the EUCC, 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 two chapters providing additional information and by annexes that define in greater details the content of the EUCS. The EUCS also defines a few specific concepts, and in particular the notion of extension profile, which is close to the notion of protection profile as used in the EUCC, and provides recommendations for future transition to and maintenance of the scheme.

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

1.2 GLOSSARY

The first sections outline the most important terminology drawn from ISO/IEC 22123-1. A more complete list of terms is defined in Annex K: (Terminology).

1.2.1 From ISO/IEC 22123-1

We will reuse the following terminology from ISO/IEC 22123-1:

Term	Abbreviations	Reference	Definition
cloud computing		3.2.1	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 Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
cloud service		3.2.2	one or more capabilities offered via cloud computing invoked using a defined interface

Term	Abbreviations	Reference	Definition
cloud deployment model		3.3.1	way in which cloud computing can be organized based on the control and sharing of physical or virtual resources Note 1 to entry: The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.
party		3.4.1	natural person or legal person, whether or not incorporated, or a group of either that can assume one or more roles
cloud service customer	CSC	3.4.2	party which is in a business relationship for the purpose of using cloud services
cloud service provider	CSP	3.4.3	party which makes cloud services available
cloud service user	CSU	3.4.4	natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services <i>NOTE:</i> Examples of such entities include devices and applications.
activity		3.4.8	specified pursuit or set of tasks
secondary cloud service provider		3.4.9	cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services
functional component		3.4.10	functional building block needed to engage in an activity , backed by an implementation
role		3.4.11	set of activities that serves a common purpose
cloud service developer		3.4.14	cloud service partner with the responsibility for designing, developing, testing and maintaining the implementation of a cloud service
measured service		3.5.1	metered delivery of cloud services such that usage can be monitored, controlled, reported and billed
tenant		3.5.2	one or more cloud service users sharing access to a set of physical and virtual resources

Term	Abbreviations	Reference	Definition
multi-tenancy		3.5.3	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		3.5.4	feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider
resource pooling		3.5.5	aggregation of a cloud service provider's physical or virtual resources to serve one or more cloud service customers
cloud capabilities type		3.6.1	classification of the functionality provided by a cloud service to the cloud service customer , based on resources used Note 1 to entry: The cloud capabilities types are application capabilities type , infrastructure capabilities type and platform capabilities type .
application capabilities type		3.6.2	cloud capabilities type in which the cloud service customer can use the cloud service provider's applications
infrastructure capabilities type		3.6.3	cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources
platform capabilities type		3.6.4	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 .
cloud service customer data	CSC data	3.10.1	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

Term	Abbreviations	Reference	Definition
			<p>NOTE 1 – An example of legal controls is copyright.</p> <p>NOTE 2 – It may be that the cloud service contains or operates on data that is not <i>cloud service customer data</i>; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available 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 <i>cloud service customer data</i>, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.</p>
cloud service derived data		3.10.2	<p>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</p> <p>NOTE – <i>Cloud service derived data</i> 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.</p>
cloud service provider data	CSP data	3.10.3	<p>class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider</p> <p>NOTE – <i>Cloud service provider data</i> 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.</p>
account data		3.10.4	<p>class of data specific to each cloud service customer that is required to administer the cloud service</p> <p>Note 1 to entry: Account data is typically generated when a cloud service is purchased</p>

Term	Abbreviations	Reference	Definition
			and is under the control of the cloud service provider . Note 2 to entry: Account data consists of data elements provided by the cloud service customer , such as; name, address, telephone, etc.
transparency		3.10.13	open, comprehensive and understandable presentation of information [SOURCE:ISO 21931-2:2019, 3.33]
inter-cloud computing		3.12.1	paradigm for enabling the interworking between two or more cloud service providers . [SOURCE: Recommendation ITU-T Y.3511, 3.2.1]
primary cloud service provider		3.12.2	In inter-cloud computing, a cloud service provider which is making use of cloud services of secondary cloud service providers as part of its own cloud services [SOURCE: Recommendation ITU-T Y.3511, 3.2.2]
secondary cloud service		From 3.12.3	cloud service of one cloud service provider which is used as part of a cloud service of one or more other cloud service providers NOTE: In ISO/IEC 22123-1, the term used is peer cloud service provider, which may lead to confusion in the context of the EUCSA.

We will in general not use the terminology from ISO/IEC 22123-1 that is not included in the table above. More specifically, the following terminology should be avoided in the definition of the EUCS:

Term	Rationale
[XX]aaS IaaS, PaaS, SaaS, ...	These “as a Service” correspond to the cloud service categories, which are too specific. Cloud capabilities types should be used instead in the EUCS. 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 EUCS, 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	a body that performs conformity assessment activities including calibration, testing, certification and inspection
EUCS Extension Profile	CSEP	A document defining extended requirements to complement the EUCS in a specific context
	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 (EUCSA, Article 58)
Stakeholder Cybersecurity Certification Group	SCCG	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders (EUCSA, Article 22)

A far more complete terminology of certification and cloud-related terms is included in Annex K: (Terminology), which is used throughout this draft document. The terms from this terminology are indicated in the present document by using a specific underlined style.

1.3 ORGANIZATION OF THE DOCUMENT

This document contains 25 more chapters and many annexes. Most chapters address a question raised in the EUCSA's Article 54(1), with two specific chapters on additional topics and on comments about the adoption and maintenance of the scheme.

The chapters usually contain two sections, with the first one being the scheme content itself, and the second one a rationale beyond this content. Each section starts with references to the Cybersecurity Act or other official documents, identified with a blue background.

Each Annex contains details about a specific part of the scheme, without any specific structure, except an introductory page that links the Annex back to the main chapters that refer to it and include any information relevant for the reader.

Finally, this is not a final version of the candidate scheme, so there are a few notes from the editor in the document to draw the attention of readers to elements of particular importance.

2. SUBJECT MATTER AND SCOPE

ARTICLE 54 REFERENCE

Article 54(1). 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 EUCS 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 shall cover any type of ICT service, provided that:

- The ICT service implements one or more cloud capabilities offered via cloud computing invoked using a defined interface [ISO22123-1];
- The ICT service aims at reaching the assurance level corresponding to one of the three levels 'basic', 'substantial' and 'high' of the EUCSA, following one of the evaluation levels defined in the EUCS.

This definition purposely covers a wide range of services, from large infrastructure services to small application services with limited reliance on cloud computing. ICT services matching these criteria will from now be referred to as "cloud services". The EUCS shall be applicable to all cloud services, following some principles:

- The EUCS aims at establishing the conformity of cloud services to a set of requirements corresponding to one of the evaluation levels defined in the EUCS;
- The EUCS does not distinguish between different categories of cloud services, unless explicitly stated in a specific rule or requirement;
- The EUCS aims at making core 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 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 aims at providing sufficient information to prospects and customers with adequate cybersecurity knowledge for making informed security decisions on cloud services, allowing them to fully understand and implement the documentation that defines their responsibility.

The EUCS focuses on cybersecurity aspects, and does not include requirements that would correspond to compliance requirements to other regulations, such as requirements on data protection.

In the evaluation of a cloud service, the EUCS shall support and encourage the reuse of conclusions and objective 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:

- The EUCS shall include an assessment of the dependencies, in which the assurance information available from subservice organizations is considered and compared to the requirements of the EUCS, in particular regarding the required level of assurance (see Annex B: Meta-approach for the assessment of cloud services).
- When a primary cloud service relies on a secondary cloud service certified with the EUCS, the EUCS conformity assessment shall aim at verifying that the assumptions defined in the secondary cloud service are adequately applied by the primary cloud service provider in the provision of its own cloud service, and included into the requirements defined for that primary cloud service (see Section 24.3, Composition).

Beyond composition, the EUCS covers other additional elements as foreseen by Article 54 of the EUCSA, under the conditions defined by Chapter 24, Additional Topics:

- The definition of cloud service extension profiles (CSEPs);
- The handling of force majeure cases;
- Rules for the protection of information related to cybersecurity certification;

Finally, the EUCS shall allow for the cybersecurity certification of cloud services extension profiles according to the criteria and methods defined in Chapter 8 below (Evaluation Methods and Criteria). CSEPs shall satisfy specific requirements, defined in Annex H: (Extension Profiles), to ensure that they do not conflict with the principles of the EUCS and that the requirements defined in the CSEPs can be audited with the EUCS methodology.

RATIONALE

Additional information from the Commission request to develop the scheme

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 present "rationale" section is intended to provide additional information to help understand the proposal made in the main chapter, and a similar section is included in every chapter. The content is not intended to be translated into articles of the implementing act, but may be used as a basis for recitals.

The definition of cloud computing and cloud service as provided in ISO/IEC 22123-1 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/IEC 22123-1 with all the classical properties (scalability, elasticity, shareable resources, self-service and on-demand), and that it offers a "defined interface" to its users.

The notion of cloud capability type is central and also defined in ISO/IEC 22123-1:

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).

Cloud capabilities types provide a more precise framework than the classical cloud service 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 cloud deployment models. ISO/IEC 22123-1 defines four cloud 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, we did not identify any specific need to focus on cloud deployment models in addition to cloud capabilities types to categorize cloud services.

About scoping, the most important characteristics of the EUCS are

- The EUCS is intended to be a horizontal scheme, applying requirements based on the same security objectives to all cloud services, covering the EUCSA's three assurance levels;
- The EUCS includes an EUCS Extension Profile (CSEP) mechanism that allows stakeholders to define additional requirements dedicated to a specific security problem, while keeping the EUCS requirements on controls as baseline;
- The EUCS does not aim at certifying the compliance of a cloud service to any regulation beyond the EUCSA, and in particular it does not aim at verifying compliance with GDPR³. Such compliance will have to be assessed using other mechanisms, and results obtained in the EUCS may be reused as objective evidence in such schemes. This reuse may be facilitated by the establishment of a dedicated CSEP, under the control of the concerned stakeholders, where the specific cybersecurity requirements of the regulation will have been transposed into additional requirements for the EUCS.
- The EUCS is a technical tool designed to provide information to customers and allow them to make informed decisions. As such, the EUCS only enforces restrictions on geographical location of data or processing, or on applicable laws at evaluation level CS-EL4; however, it requires the CSP to be transparent about this information at all evaluation levels, and to make it publicly available and understandable as part of the information provided with the certificate.
- The EUCS recognizes that cloud services are based on complex systems, and that many CSPs will rely on subservice providers. 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 fulfilment of relevant requirements by the subservices they provide.
- The EUCS also defines requirements for composition. When a cloud service uses a subservice that has been previously certified in the EUCS, it should be easy to reuse the results from that certification (see Section 24.3, Composition). The requirements related to composition defined in the EUCS apply to both the secondary cloud service and to the primary cloud service.

The composition process can only be used when a subservice used by the CSP has been certified through EUCS. For subservices that have not been certified through EUCS (for instance because the subservice is not a cloud service),

³ 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)

the dependency analysis process has been defined to analyse other assurance documentation (certificates, reports) in order to build assurance about how the subservice providers comply to the relevant scheme requirements.

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 customers.

POLITICO

3. PURPOSE OF THE SCHEME

ARTICLE 54 REFERENCE

Article 54(1). 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 aims at improving the EU Internal Market conditions, and at enhancing the level of cybersecurity of a wide range of cloud services, of the cloud capabilities types they implement, including application, infrastructure, and platform capabilities.

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

Users of the EUCS shall include:

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

Satisfying the needs of these user is indeed the purpose of the EUCS, with one distinct objective for each category of users:

- For CSPs. The EUCS 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 EUCS 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 EUCS shall allow Regulatory Authorities to refer to the EUCS in European and national regulations, including criteria based on information defined in the EUCS, and it shall allow them to enforce regulations by verifying the status and the information provided in the certificates stored in the web site on cybersecurity certification managed by ENISA.

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

- four (4) evaluation levels (see Chapter 5, Assurance Levels), implementing assurance levels 'basic', 'substantial' and 'high' defined in the EUCSA, which can cover cloud services corresponding to a wide range of risk appetites;
- a set of security objectives and requirements (see Chapter 8, Evaluation Methods and Criteria and Annex A., Security Objectives and requirements for Cloud Services), defining objectives to be met by CSPs for all certified cloud services, further decomposed into requirements mapped to the assurance levels referred to above;

- a conformity assessment meta-approach (see Annex B: Meta-approach for the assessment of cloud services) defining how to use one of the two conformity assessment methods to determine that a cloud service fulfils the requirements assigned to a given assurance level;
- two conformity assessment methods (see Chapter 8, Evaluation Methods and Criteria, Annex C: Assessment for levels CS-EL2 and above and Annex D: Assessment for level CS-EL1) 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 structure 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 life cycle of certificates after their issuance, including maintenance and renewal requirements, management of vulnerabilities, handling of complaints, and market surveillance activities, that may allow scheme users to stay informed of the evolution of the security of a given cloud service;
- a mechanism for defining EUCS extension profiles that would complement the EUCS requirements on controls with requirements specific to a given use case and security story.

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

- 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 CS-EL3 and CS-EL4 evaluation levels, authorisation by the national authorities and peer assessment between conformity assessment bodies;
- the flexibility offered by four different evaluation 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 ENISA's web site dedicated to EU cybersecurity certification;
- assurance maintained over time, with regular conformity assessments, including operating effectiveness guarantees at the levels CS-EL2, CS-EL3 and CS-EL4;
- a maintenance framework for the EUCS itself, endorsed by European institutions and Member States, providing strong guarantees on continued operation of the EUCS;
- integration in the European cybersecurity certification framework, which will facilitate the reuse of EUCS-certified cloud services in other European cybersecurity certification 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 EUCS's intended users cover all relevant parties in the life cycle of the certificate (production and consumption) and, due to the nature of the scheme, all relevant parties in the life cycle of the cloud service.

Table 1 and Table 2, below, describe the intended users as parties of the certificate and their role related to the EUCS. The table focuses on the main roles, but the fulfilment of all EUCS service requirements relies on additional roles, such as top management of human resources, which are described in the requirements.

Table 1: Parties involved in the production of EUCS certificates

Party	Role	Description
<u>CSP</u>	Development	The Development role covers the <u>activities</u> related to the development of the <u>cloud service</u> , including architecture design, hardware and software development, and service design. It also includes processes, in particular the development process.
<u>CSP</u>	Operations	The Operations role covers the <u>activities</u> related to the operation of the <u>cloud service</u> , 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).
<u>CSP</u>	Compliance	The Compliance role covers the <u>activities</u> related to the verification of <u>compliance</u> to standards and regulations, including <u>documentation</u> , <u>self-assessment</u> , interfaces with <u>CABs</u> , and management of EU statements of <u>conformity</u> .
<u>CAB</u>	Evaluation	The Evaluation role for <u>CABs</u> includes all the <u>activities</u> related to the <u>conformity assessment</u> of <u>cloud services</u> and related processes.
<u>CAB</u>	Review and Certification	The Review and Certification role for <u>CABs</u> includes all the activities related to the <u>issuance</u> and management of <u>certificates</u> , including in particular the <u>review</u> of the <u>evaluation</u> and of its results.
<u>NCCA</u>	As a CAB	For assurance level 'high', the NCCA is involved and may take the role of a <u>CAB</u> . This would include at least the Review and Certification role, and it may also include the Evaluation role.
<u>NCCA</u>	Compliance monitoring	NCCAs are in charge of supervising the implementation of EU cybersecurity <u>certification schemes</u> , including a Compliance Monitoring role, to ensure that <u>certified cloud services</u> remain <u>compliant</u> to the <u>requirements</u> of the EUCS.
<u>NAB</u>	CAB Accreditation	NABs are not directly involved in the production of <u>certificates</u> , but their role in the <u>accreditation</u> of <u>CABs</u> is essential in the proper operation of the EUCS
<u>ENISA</u>	Publicity	ENISA is in charge of publicizing the <u>certificates issued</u> in the context of the EUCS, as well as the events associated with these certificates.

Table 2: Stakeholders consuming EUCS certificates

Party	Role	Description
<u>CSC</u>	Procurement	The Procurement role covers the <u>activities</u> related to the selection of a <u>cloud service</u> , and in particular the definition of the criteria and the assessment of the candidates, leading to the selection.
<u>CSC</u>	Customer Development	The Customer Development role covers the <u>activities</u> related to the development of new products or services on the basis of the <u>certified cloud service</u> , possibly including other cloud services. Developers will in particular rely on the recommendations provided with the <u>certified cloud service</u> .

Party	Role	Description
CSC	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.
CSC	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 objective evidence or conclusions generated during the cloud service evaluation.
CSU	User	The User role is limited, since Cloud Service Users are not expected here to be primary users of the EUCS, but they should be targeted as secondary users through CSCs. Users are nevertheless directly targeted by some of the documentation provided by the CSP and evaluated in the context of the EUCS, 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 EUCS as a basis for including high-level requirements (mandatory certification) or more detailed requirements, for instance building on transparency requirements. The Regulation role may also include the development of extension profiles corresponding to these rules and regulations.
Regulatory authority	Enforcement	The Enforcement role includes all activities related to the enforcement of regulations that mention the EUCS. Enforcers will in particular need to verify that CSPs comply with the parts of the regulation that depend on the EUCS.

Out of the parties 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 EUCS.

Cloud Service Users (the actual persons or devices 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 EUCS, 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 certain knowledge in cybersecurity that cannot by default 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. These users may use the EUCS:

- to assess how a cloud service, as described by the CSP, meets the requirements related to a predefined set of security objectives and controls, when used according to security recommendations provided by the CSP;
- to provide CSCs the information required to make informed decisions 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 EUCS in European and national regulations, including criteria based on information defined in the EUCS, and allow them to presume compliance with the cybersecurity requirements defined in the specific regulation upon verification of the certification in the ENISA cybersecurity certification website.

For CSPs, the EUCS offers:

- a single certification scheme recognized across the entire European Union;
- four evaluation levels corresponding to different needs from the CSPs and different use cases;
- two conformity 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 evaluation 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 EUCS.

For CSCs, the EUCS offers:

- a single certification scheme recognized the entire European Union;
- four evaluation 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 EUCS offers:

- a single certification scheme recognized the entire European Union;
- four evaluation 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(1). 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 EUCS relies on a number of standards and technical specifications:

- International standards ISO/IEC 22123-1 and ISO/IEC 17000, and when needed ISO/IEC 9000 and ISO/IEC 27000, shall be used as references for the terminology used through the scheme, complementing with input from all the standards and schemes listed below when required.
- The EUCS service requirements are defined in an Annex of the present scheme (see Annex A.: Security Objectives and requirements for Cloud Services). These service requirements are based on the security controls defined in international standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, and on documents previously issued by Member States to define the security controls and associated requirements in their respective National Schemes [C5, SecNumCloud, ZekerOnline].
- The definition of the evaluation levels reuses some concepts defined in the ISO/IEC 15408-3 standard.
- The conformity assessment methodology defined in the EUCS shall be based on the ISO/IEC 17065 harmonized standard, and it will be complemented by additional requirements for the accreditation of CABs to be developed in collaboration with CEN-CENELEC.
- The requirements for CABs performing vulnerability identification and penetration testing shall be based on the ISO/IEC 17025 harmonized standard, which will be complemented by additional requirements for the accreditation of CABs performing these activities, to be developed later as guidance by ENISA in collaboration with the ECCG.

The EUCS also leverages several conformity assessment methods and standards:

- International standards ISO/IEC 17021-1 and ISO/IEC 27006.
- International standards on assurance engagements ISAE 3402 and ISAE 3000.
- Two methods defined in Annexes to the present scheme (see Annex B.: Meta-approach for the assessment of cloud services, Annex C.: Assessment for levels CS-EL2 and above and Annex D.: Assessment for level CS-EL1).

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/IEC 27005 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 this Regulation:

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.



The standards that are referenced are very classical in the IT security field, but in most cases, it has not been possible to apply the standards directly, and new specifications have been defined.

In addition, 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 currently operate National Schemes for cloud services.

For the conformity assessment methods, the EUCS recognizes the two most widely used assessment method families (based on the ISO/IEC 17000 family and on the ISAE 3000 family), but there has been a need to define a methodology drawing from both families for assurance levels 'substantial' and 'high', and to add a specific and simplified assessment method for the 'basic' assurance level, which are defined in annexes to the scheme.

Both documents have been written in a way that could allow them to be considered as a basis for the establishment of new Technical Specifications or standards. The security controls defined in Annex A: (Security Objectives and requirements for Cloud Services) are for most of them⁴ under discussion in CEN-CENELEC JTC13's WG2⁵ to define a Technical Specification⁶.

⁴ The requirements on Cloud Service Extension Profiles, as well as some requirements that explicitly mention the EU are defined in the present document.

⁵ Following approval by CEN-CENELEC JTC13 of the New Work Item on "Multi-layered approach for a set of information security requirements for information/cyber security controls for Cloud Services".

⁶ If the Technical Specification is available before the Implementing Act derived from this candidate scheme reaches the comitology discussions phase, these requirements may be replaced by a reference to this Technical Specification.

5. ASSURANCE LEVELS

ARTICLE 54 REFERENCE

Article 54(1). A European cybersecurity certification scheme shall include at least the following elements:

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



The EUCS shall support the three assurance levels defined in the EUCSA. In order to meet the requirements of the 'basic' assurance level of the EUCSA, a cloud service shall be certified against evaluation level CS-EL1 of the present scheme. In order to meet the requirements of the 'substantial' assurance level of the EUCSA, a cloud service shall be certified against evaluation level CS-EL2 of the present scheme. In order to meet the requirements of the 'high' assurance level of the EUCSA, a cloud service shall be certified against evaluation level CS-EL3 or CS-EL4 of the present scheme.

As specified in the EUCSA's Article 52(5) for the 'basic' assurance level, evaluation level CS-EL1 is "intended to minimise the known basic risks of incidents and cyberattacks" and can be further defined as follows:

- Evaluation level CS-EL1 shall provide limited assurance through evaluation by a CAB that the cloud service is built and operated with procedures and mechanisms to meet the service requirements pertaining to evaluation level CS-EL1 at a level intended to minimize the known basic risks of incidents and cyberattacks.
- Evaluation level CS-EL1 shall 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 evaluation level CS-EL1 shall 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 evaluation level CS-EL1 shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to assurance level CS-EL1, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including on the processes and on the functional components (understood as result of a development process) underlying the service.
- The evaluation depth for evaluation level CS-EL1 shall consist mostly of documentation review activities, based on a check for sufficiency and appropriateness of the evidence gathered by the CSP during an internal audit on processes and design intended to confirm the fulfilment of requirements by technical and organisational controls and the existence of these controls, including requirements for testing of basic known vulnerabilities and automated compliance checks by the CSP.
A report following defined procedures shall be generated by the CAB.
Once a cloud service is certified, internal audit results shall be regularly updated and submitted to the CAB to justify the continued development and operation of the service in compliance with the requirements of the evaluation level.
- The evaluation depth for evaluation level CS-EL1 shall be driven by a predefined audit plan supported by a questionnaire.

As specified in the EUCSA's Article 52(6) for the 'substantial' assurance level, evaluation level CS-EL2 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:

- Evaluation level CS-EL2 shall 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, has implemented suitable controls that, if operating effectively, minimise those risks and allow the cloud service to fulfil the service requirements, pertaining to evaluation level CS-EL2, and have operated these controls effectively throughout a specified period.

- Evaluation level CS-EL2 shall 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 evaluation level CS-EL2 shall 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 evaluation level CS-EL2 shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to assurance level CS-EL2, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including on the processes and on the functional components (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 evaluation level CS-EL2 shall include, in addition to the scope for evaluation level CS-EL1, 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 CS-EL2 shall include limited penetration testing activities using known attacks.

As specified in the EUCSA's Article 52(7) for the 'high' assurance level, evaluation level CS-EL3 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:

- Evaluation level CS-EL3 shall 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, if operated effectively, minimise those risks and allow the cloud service to fulfil the service requirements pertaining to evaluation level CS-EL3, and have operated these controls effectively throughout a specified period.
- Dedicated requirements are defined in Annex A: (Security Objectives and requirements for Cloud Services) to ensure that essential 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.
- Evaluation level CS-EL3 shall 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 evaluation level CS-EL3 shall 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 evaluation level CS-EL3 shall be defined by the description of the cloud service and by the security objectives and requirements pertaining to evaluation level CS-EL3, as defined in Annex A: (Security Objectives and requirements for Cloud Services), including on the processes and on the functional components (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 level CS-EL3 shall include an assessment of the resistance to skilled attackers through vulnerability identification and penetration testing activities performed by a CAB whose independence and qualification about penetration testing has been demonstrated through accreditation and authorisation.
- The evaluation scope for level CS-EL3 shall include an assessment of the independence from non-EU law of the cloud service, including in particular requirements about a risk assessment by the CSP of their exposure to non-EU law, about the location of storage and processing of CSC data, and about controls on employees or suppliers accessing this data from outside of the EU, as defined in Annex J: (Protection of European data against unlawful access).
- The evaluation depth for evaluation level CS-EL3 shall be based on the depth for evaluation level CS-EL2, 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 essential 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 evaluation level CS-EL3 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 requirements on security controls pertaining to evaluation level CS-EL3.

As specified in the EUCSA's Article 52(7) for the 'high' assurance level, evaluation level CS-EL4 is also "intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources", but it only targets the most sensitive cloud services, and more specifically those that process data, whether personal or not, of particular sensitivity, and the breach of which is likely to result in a breach of public order, public safety, human life or health, or the protection of intellectual property. The differences with level CS-EL3 are as follows:

- The evaluation scope for evaluation level CS-EL4 shall include an assessment of the independence from non-EU law of the cloud service, including in particular requirements about the effective control of the CSP, about the location of storage and processing of CSC data, and about controls on employees or suppliers accessing this data from outside of the EU, as defined in Annex J: (Protection of European data against unlawful access).

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.

Rationale overview

All [evaluation levels](#) defined in the EUCS satisfy all [requirements](#) that are applicable to the corresponding EUCSA [assurance level](#):

- Every evaluation 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 evaluation level defines service requirements and functionalities, as well as the rigour and depth required in the evaluation (Article 52(3)).
- Every evaluation level requires that evaluation activities include a review of technical documentation (Article 52(5), Recital 67).
- Every evaluation level requires a review of the cloud service's main processes, including the development process used for the development of the cloud service (Recital 88).

Those are the only requirements defined for assurance level 'basic' in the EUCSA, which are all satisfied by evaluation level CS-EL1.

In addition, there are more requirements pertaining to the EUCSA's assurance level 'substantial':

- The requirements on security controls for assurance level 'substantial' include a vulnerability assessment activity that perform a review of publicly known vulnerabilities (Article 52(6)).
- The requirements on security controls for assurance level 'substantial' 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 89).

These requirements are all met by evaluation level CS-EL2, which is mapped to the EUCSA's assurance level 'substantial':

Finally, there are a few more requirements pertaining to the EUCSA's assurance level 'high':

- The requirements on security controls for assurance level 'high' include a vulnerability assessment activity that perform a review of publicly known vulnerabilities (Article 52(7)).
- The requirements on security controls for assurance level 'high' include a review of the functional tests of the cloud service's security functionalities, as well as automated monitoring requirements, (Article 52(7)).
- The requirements on security controls for assurance level 'high' include the use of state-of-the-art security functionalities, including requirements on the independence of CSPs from non-EU laws (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 89).
- The assessment methodology for assurance level 'high' mandates both design efficiency and operating efficiency to be assessed during the evaluation (Recital 90). This assessment includes penetration testing to assess the resistance of security functionalities of the cloud services; in addition, some of the penetration testing shall be performed by an accredited and authorised entity (Article 52(7), Recital 90).

There are in the EUCS two evaluation levels mapped to the EUCSA's assurance level 'high', which differ mostly by their handling of requirements on independence from non-EU law (see Annex J:, Protection of European data against unlawful access):

- Certification level CS-EL3 is intended for use cases where independence from non-EU law is an important factor, but to a level that may vary between CSCs, depending on their precise use case and legal structure; this level therefore includes technical and contractual aspects, but only includes transparency requirements related to some other aspects, in particular related to the effective control of the CSP by non-EU legal entities.
- Certification level CS-EL4 is intended for the most sensitive uses of cloud services, which are defined by the sensitivity of data to be processed by the cloud service, and more specifically to the potential negative impact that a breach of this data may have on public order, public safety, human life or health, or the protection of intellectual property. Certification level CS-EL4 mostly adds requirements related to the effective control of the CSP by non-EU legal entities.

Note that, throughout this document, references to the assurance levels defined in the EUCSA use lowercase and quotes ('basic', 'substantial', 'high'), whereas the evaluation levels defined in the EUCS are capitalized and prefixed (CS-EL1, CS-EL2, CS-EL3, CS-EL4). The names assigned to evaluation levels in the EUCS may be later modified.

POLITICO

DETAILED PRESENTATION

This section provides a full background on the definition of the EUCS [evaluation levels](#).

PARAMETERS

Intention

The intention parameter provides a general description of the [evaluation levels](#), typically matching closely the definition from the [assurance levels stipulated in the EUCSA](#).

Suitability

Suitability is about potential restrictions of the [cloud capabilities 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 CS-EL3 [evaluation level](#). Cybersecurity [certification](#) cannot provide guarantees of resistance against the most highly skilled and resourceful teams of attackers determined to target a specific service 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 [cloud 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.*, all requirements of a lower [evaluation level](#) are similarly included in the depth of the higher [evaluation 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 EVALUATION LEVELS

Level	CS-EL1	CS-EL2	CS-EL3	CS-EL4
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 service 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 operated effectively, minimize those risks and meet the corresponding service requirements, and has operated these controls effectively throughout a specified period.	Provide reasonable assurance through evaluation by an independent third-party 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, if operated effectively, minimize those risks and meet the corresponding service requirements, and has operated these controls effectively throughout a specified period. Security controls are monitored for continuous operation in accordance with their design; they are structurally reviewed and pen tested to validate their actual ability to prevent or detect security breaches.	Provide reasonable assurance through evaluation by an independent third-party 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, if operated effectively, minimize those risks and meet the corresponding service requirements, and has operated these controls effectively throughout a specified period. Security controls are monitored for continuous operation in accordance with their design; they are structurally reviewed and pen tested to validate their actual ability to prevent or detect security breaches.
Intention rationale	Scope, depth and rigour of the evaluation level is limited to procedures and mechanisms for those service requirements that shall minimize basis risks only.	Scope, depth and rigour of this evaluation level requires the CSP to apply a risk-based approach for the suitable design and implementation of controls that meet the corresponding service 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 evaluation level extend the level for CS-EL2 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. Structural 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.	Scope, depth and rigour of this evaluation level extend the level for CS-EL3 by additional procedures to be performed for assessing the independence of the CSP from interference from states that are not EU Member States.
Suitability	The evaluation level CS-EL1 is suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems.	The evaluation level CS-EL2 is suitable for cloud services that are designed to meet typical security requirements on services for business-critical data and systems.	The evaluation level CS-EL3 is suitable for cloud services that are designed to meet specific (exceeding assurance level CS-EL2) security requirements on services for mission critical data and	The evaluation level CS-EL4 is suitable for cloud services that process data, whether personal or not, of particular sensitivity, and the breach of which is likely to result in a breach of public



Level	CS-EL1	CS-EL2	CS-EL3	CS-EL4
			systems, including those related the fundamental interest to society.	order, public safety, human life or health, or the protection of intellectual property.
Suitability rationale	The CS-EL1 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 CS-EL1 level demonstrates a willingness to address security, including the application of security guidance from subservice providers.	The CS-EL2 level provides reasonable assurance that a set of more stringent (than in level CS-EL1) 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 cloud capabilities types. The CS-EL2 level demonstrates a robust and mature holistic security management to provide secure services.	The CS-EL3 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. The costly and rigorous evaluation process reflects the intention to minimize the risks in using the cloud service.	The CS-EL4 level provides reasonable assurance that a set of security controls is designed and operated in a way that goes beyond the CS-EL3 level to address security risks and threats related to data of particular sensitivity that would present risks to society if breached. The data of particular sensitivity mentioned above cover: - data related to secrets protected by law, for example, secrets relating to the deliberations of the Government and of the authorities reporting to the executive branch, to national defense, to foreign policy, to national security, to proceedings before the courts, or to the protection of privacy, to medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies; - data that are necessary for the accomplishment of essential State functions, in particular the safeguarding of national security, the maintenance of public order and the protection of human life and health.
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.	Team of highly skilled persons with access to significant resources, possibly including the resources of a state. to design and perform attacks, get insider attacks, discover or buy access to previously unknown vulnerabilities.



Level	CS-EL1	CS-EL2	CS-EL3	CS-EL4
Attacker profile rationale	<p>Today, the CS-EL1 level 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.</p> <p>When such certification becomes mainstream, the requirements should be revised upwards.</p>	<p>This is the “standard” attacker, corresponding to most real-life attacks used to disclose information, steal resources, deny service, or tamper with a service.</p> <p>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.</p>	<p>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.</p>	<p>This is also a sophisticated attacker, but the possible access to state resources, including through laws of this state that may conflict with EU laws, requires mitigation through risk avoidance.</p> <p>This attacker profile covers hybrid threats, where hostile states outside of the EU may target cloud services provided to EU Member States and citizens.</p>
Scope	<p>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.</p>	<p>As defined by the service description and the controls pertaining to the CS-EL2 level, including processes and the software (understood as result of a development process) underlying the service.</p> <p>Operating effectiveness of the controls shall be demonstrated.</p>	<p>As defined by the service description and the controls pertaining to the CS-EL3 level, including processes and the software (understood as result of a development process) underlying the service.</p> <p>Operating effectiveness of the controls shall be demonstrated. (including automated monitoring if required by the control definition).</p> <p>Specific controls are used to assess the level of possible interference from non-EU states.</p>	<p>As defined by the service description and the controls pertaining to the CS-EL4 level, including processes and the software (understood as result of a development process) underlying the service.</p> <p>Operating effectiveness of the controls shall be demonstrated. (including automated monitoring if required by the control definition).</p> <p>Specific controls are used to mitigate possible interference from non-EU states.</p>
Scope rationale	<p>The scope includes all controls, but with a minimal set of requirements, to ensure that the CSP has defined and implemented security controls, with limited constraints and requirements.</p>	<p>We refer to the same controls from the CS-EL1 evaluation level, but with the stronger refinements or enhancements (e.g., (mandated techniques, thresholds, etc.).</p> <p>Requirements must include a limited penetration testing using known attacks.</p>	<p>We refer to the same controls from the CS-EL2 evaluation level, but with the higher refinements or enhancements.</p> <p>Enhancements include additional constraints, references to state-of-the-art requirements, and automated monitoring of some controls. Penetration testing requirements are also much more precise, and requirements on assessment of exposure to interference from non-EU states are defined.</p>	<p>We refer to the same controls from the CS-EL3 evaluation level, but with the complementary requirements.</p> <p>The new requirements include additional constraints on the location of data processing and on the exposure of cloud service providers to interference from non-EU states.</p>
Depth	<p>Document review solely, based on a check for completeness and coherence of the provided internal audit results and of the associated documentation on processes and design intended to</p>	<p>Additional to the requirements of CS-EL1: On-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified policies and</p>	<p>Additional to the requirements of CS-EL2: Specific requirements on the monitoring and testing of the controls, i.e. their operation as intended to</p>	<p>The depth of assessment is similar to this of the CS-EL3 level.</p> <p>The depth of the legal analysis performed relatively to possible</p>



Level	CS-EL1	CS-EL2	CS-EL3	CS-EL4
	<p>confirm meeting technical and organizational measures, and interactions between the auditor and the CSP at the beginning and at the conclusion of the conformity assessment.</p> <p>A report following defined procedures is generated by the CAB.</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>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>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 carried out by accredited and authorised third-parties, following a multi-year plan that needs to be validated in the audit.</p>	<p>influence from non-EU states is the major difference.</p>
Depth rationale	<p>The third-party audit focuses on completeness, coherence and plausibility of the internal audit results and related 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 controls to protect the operation of 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 CS-EL2 level.</p> <p>The main addition in depth come from additional requirements for the 'high' level, such as automated monitoring and penetration testing, which are intended to demonstrate that the controls remain effective under strenuous conditions.</p>	<p>The audit aims at providing the same reasonable assurance as for the CS-EL2 and CS-EL3 levels.</p>
Rigour	<p>An internal audit is performed by the CSP and driven by a predefined checklist.</p> <p>An accredited third-party then audits the internal audit 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 CS-EL2 level, but the CAB needs to be authorised by the NCCA to it has the required competencies to audit the specific requirements of the CS-EL3 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> <p>A specifically accredited and authorised CAB needs to be involved in the performance of vulnerability identification and penetration testing activities.</p>	<p>The assessment is performed as for the CS-EL2 level, and the CAB needs to be authorised by the NCCA, like for the CS-EL3 level.</p> <p>The competencies required for the CAB will be slightly different, in particular regarding the deeper legal analysis required.</p>



Level	CS-EL1	CS-EL2	CS-EL3	CS-EL4
Rigour rationale	The assessment follows all items in a checklist suited to the targeted cloud service, and its results are reviewed by an accredited third-party .	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>The rigour remains mostly the same as for level CS-EL2, 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> <p>The addition of testing by a CAB provides an additional level of rigour around the critical activities of vulnerability identification and penetration testing.</p>	The rigour remains mostly the same as for levels CS-EL2 and CS-EL3



6. SELF-ASSESSMENT

ARTICLE 54 REFERENCE

Article 54(1). 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.

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 CSPs could only have been allowed for all cloud services that present a low risk (Article 53(1) of the EUCSA), *i.e.*, to a subset of the cloud services that could be certified at evaluation level CS-EL1.

The Ad Hoc Working Group consistently expressed that self-assessment was not suitable for cloud services, even at level CS-EL1 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 service requirements, that are entirely new. Rather than allowing CSPs to interpret these service requirements, it is preferable to only allow accredited CABs to use the EUCS, 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 of 2020, 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 EUCS.

POLITICO

7. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

ARTICLE 54 REFERENCE

Article 54(1). 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 issuing certificates in the context of the EUCS shall be accredited for [ISO17065], complemented by the requirements defined for the EUCS (see Annex E:, Competence requirements for CABs).

ENISA may provide, with the support of the European co-operation for Accreditation, and in cooperation with the ECCG, guidance for harmonised interpretation of ISO/IEC 17065 for the accreditation of CABs for the EUCS, also considering related relevant standards such as ISO/IEC 17021-1.

For the evaluation levels CS-EL3 and CS-EL4, the evaluation activities shall include penetration testing activities. All CABs performing such test activities in the context of the EUCS shall be accredited for [ISO17025], complemented by the requirements defined for the EUCS (see Annex E:, Competence requirements for CABs).

For the evaluation levels CS-EL3 and CS-EL4, the evaluation activities shall include the audit of a risk assessment on the impact of non-EU laws, which will require specific legal competences, combined with financial competences for the audit of the requirements about control from non-EU entities (see Annex E:, Competence requirements for CABs).

With the support of the European co-operation for Accreditation, and in cooperation with the ECCG, ENISA may provide guidance for harmonised interpretation of relevant standards, such as ISO/IEC 17020 or ISO/IEC 17025, for the accreditation of testing laboratories for the EUCS.

Additional requirements

For the evaluation levels CS-EL3 and CS-EL4, in addition to the accreditation of the CAB according to ISO/IEC 17065, the EUCS scheme provides for the following specific requirements to which CABs are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements:

- specific requirements shall concern technical competences related to specific conformity assessment activities and shall apply only as regards certificates issued at evaluation levels CS-EL3 and CS-EL4;
- requirements shall apply both to internal personnel of CABs and to the external ones in cases where conformity assessment activities are performed by a subcontractor.

These CABs and their concerned personnel shall be required to meet the following requirements:

- to have the necessary expertise and experience in designing and analysing the specific testing activities to determine the cloud service's resistance against specific attacks (penetration testing) on the operation of the cloud service by an attacker with significant skills and resources;

- to have the necessary expertise and experience in performing reviews of the design and implementation of security measures in cloud services, and in performing architecture reviews of the systems providing a cloud service.

Also for the evaluation levels CS-EL3 and CS-EL4, in addition to the accreditation of testing laboratories according to ISO/IEC 17025, personnel performing test activities shall have the necessary expertise to perform specific testing activities to determine the cloud service's resistance against specific attacks (penetration testing) by an attacker with significant skills and resources on the operation of the cloud service.

Finally, for the evaluation level CS-EL4, CABs performing the certification and their personnel shall be required to meet the following requirements:

- to have the necessary expertise and experience in analysing the legal and financial information provided by the CSP relatively to the risk assessment on possible interference from non-EU laws.

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

Notification

For each CAB issuing certificates notified in accordance with Article 61 of the EUCSA, the notification shall include:

- the highest EUCSA assurance level ('substantial' or 'high') and EUCS evaluation level (CS-EL2, CS-EL3 or CS-EL4) for which the CAB is allowed to issue certificates;
- where applicable, the list of the subcontractors performing evaluation activities for the CAB, including the evaluation level up to which each subcontractor can evaluate.

Authorisation

A NCCA shall, for the authorisation of a CAB to carry out activities at evaluation levels CS-EL3 and CS-EL4 under the EUCS scheme, proceed to the assessment of the compliance with the additional requirements described above of the CAB, including any of its subcontractors performing evaluation activities.

This assessment shall include:

- conducting structured interviews to determine that the CAB and its personnel have the necessary expertise and experience in the relevant activities;
- reviewing the objective evidence of pilot evaluation performed as part of the accreditation procedure of the CAB and evaluating their performance.

In cases where evaluation activities are performed by a subcontractor, authorised CABs shall provide the necessary technical support to their NCCA for the assessment of the subcontractors, and shall participate to their audit on a regular basis (at least every two (2) years).

This support shall also cover the assessment that the subcontractors meet the stringent security requirements necessary for the protection of sensitive or protected information relating to cloud services under evaluation and to the process of evaluation itself, as requested by Section 24.2 (Security of Information).

Unless duly justified, authorised CABs shall participate and provide technical support to the maintenance of the scheme.

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;

Article 56(6) provides further information on delegation at assurance level 'high', and Article 60 defines how the requirements defined here should be used:

Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:

(a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or

(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

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 it is not reproduced here.

The general competences required for CABs are rather generic, since most of the controls are related to the processes used by the CSP. Nevertheless, some controls require additional competences, in particular at the highest evaluation level, which will be subject to authorisation by a NCCA.

Penetration testing and analysis of development activities and system configurations are included as additional competence requirements for all CABs performing conformity assessment activities at evaluation levels CS-EL3 and CS-EL4, since those activities do require specific competences, but the "including" formulation does not preclude the addition of further activities.

Regarding penetration testing and related activities for the CS-EL3 and CS-EL4 evaluation levels, there are two types of CABs, to which correspond two different categories of additional competence requirements to be evaluated as part of the authorisation process:

- A CAB issuing certificates and performing audits, accredited to ISO/IEC 17065, is required to have sufficient knowledge to design and analyse vulnerability identification and penetration testing activities;
- A CAB performing test activities, accredited to ISO/IEC 17025, is required to have sufficient knowledge to design and perform vulnerability identification and penetration testing activities.

For the assessment of the capabilities of a CAB to perform evaluations at the CS-EL3 and CS-EL4 evaluation levels, no detailed harmonised framework has been set up so far, although NCCAs proceed in general to this assessment considering:

- the experience of the [CAB](#) and associated personnel;
- their capabilities to determine the service's resistance against attacks by skilled attackers ([penetration testing](#));
- the necessary interviews and/or tests of the auditors, and the possible close [monitoring](#) by the [NCCA](#) of pilot [evaluations](#) at the CS-EL3 and CS-EL4 [evaluation levels](#).

As a consequence, the harmonisation of the way to perform this assessment for this first version of the EUCS is to be achieved through the peer review mechanism and ENISA may further develop in cooperation with the ECCG guidance based on these peer reviews/assessments.

The rules for [authorisation](#) and notification have also been added in this chapter. They are rather basic of nature, as [authorisation](#) is about verifying the [compliance](#) to the additional [competence requirements](#) defined earlier in this chapter. A few details have been added for subcontractors. The most important is here that the subcontractors are included in the [authorisation process](#) and must be declared in the [notification processes](#).

POLITICO

8. EVALUATION METHODS AND CRITERIA

ARTICLE 54 REFERENCE

Article 54(1). 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 evaluation criteria defined in Annex A: (Security Objectives and requirements for Cloud Services) shall be applied for the certification of cloud services according to the EUCS.

The EUCS assessment methodology, based on the [ISO17065] standard and defined in Annex B: (Meta-approach for the assessment of cloud services), shall be applied for the certification of cloud services according to the EUCS, together with the appropriate conformity assessment approach, depending on the targeted evaluation level:

- The assessment approach that shall be used for evaluation levels CS-EL2 and above is defined in Annex C: (Assessment for levels CS-EL2 and above), and it draws inspiration from both the [ISO17021] standard and from the ISAE family of standards [IAASB Handbook];
- The evidence-based assessment approach that shall be used solely for evaluation level CS-EL1, is defined in Annex D: (Assessment for level CS-EL1),.

These approaches will be complemented by harmonized interpretations of the ISO/IEC 17065 standard in the context of EUCS, to be developed by ENISA with the support of the European co-operation for Accreditation (EA) and in cooperation with CEN-CENELEC. When available, these harmonized interpretations shall be applied.

In addition, for evaluation levels CS-EL3 and CS-EL4, ENISA will develop a harmonized interpretation of the ISO/IEC 17025 standard in the context of EUCS with the support of the European co-operation for Accreditation (EA), and in cooperation with the ECCG. When available, these harmonized interpretations shall be applied.

Objectives of Article 51 of the EUCSA shall be covered by the strict application of the security objectives and requirements defined in Annex A: (Security Objectives and requirements for Cloud Services). Table 3 below provides a high-level mapping of the coverage of requirements posed by this Article 51 by security categories from Annex A:.

The certification of EUCS extension profiles shall be performed using the assessment approach defined in Annex C: (Assessment for levels CS-EL2 and above), using the specific criteria defined in Annex H: (Extension Profiles), which also provides additional details about this specific certification process.

Table 3: Coverage of Article 51 of the EUCSA 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,	This is covered in many control categories, including in particular the CKM category (covering cryptography) and the

Security objectives from Article 51	Categories from Annex A:
access or disclosure during the entire life cycle of the <u>ICT product</u> , <u>ICT service</u> or <u>ICT process</u> ;	CS category (covering the security of communications), as well as the PUA category (independence from non-EU laws)
(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 <u>ICT product</u> , <u>ICT service</u> or <u>ICT process</u> ;	This is covered in many <u>control</u> categories, 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 <u>access rights</u> refer;	This is covered in particular by the IAM category (covering identity management, authentication, and <u>access control</u>), complemented by some requirements from the HR category on human resources management
(d) to identify and document known dependencies and <u>vulnerabilities</u> ;	This is covered by the PM category (defining relationships with suppliers) and the OPS category (defining <u>vulnerability handling</u>)
(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;	This is 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 covered by the OPS category (defining logging)
(g) to verify that <u>ICT products</u> , <u>ICT services</u> and <u>ICT processes</u> do not contain known <u>vulnerabilities</u> ;	This is covered by the OPS category (defining general <u>vulnerability identification</u> 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 covered by the BCM category (defining business continuity) and the PS category (defining physical security measures)
(i) that <u>ICT products</u> , <u>ICT services</u> and <u>ICT processes</u> are secure by default and by design;	This is covered in the DEV category (defining methodology), with complements in many other categories
(j) that <u>ICT products</u> , <u>ICT services</u> and <u>ICT processes</u> are provided with up-to-date software and hardware that do not contain publicly known <u>vulnerabilities</u> , and are provided with mechanisms for secure updates.	This is covered by the OPS category (<u>vulnerability handling</u>), 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 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 EUCS 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] standard 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.

The requirements on security controls are currently under discussion at CEN-CENELEC in order to become Technical Specifications. It is expected that most of the requirements, if not all, will be defined in these Technical Specifications. However, the references to Annex A have been kept because the annex will remain the reference for EUCS requirements, whether they are listed in that Annex, in another Annex, or in an external document. Some requirements



are not suited for inclusion in a CEN-CENELEC Technical Specification, so there are additional and EUCS-specific requirements, such as those defined today in Annex J: (Protection of European data against unlawful access), and there may also be a need to provide additional requirements or clarifications about these Technical Specification.

Finally, in the present version of the draft candidate scheme, as the Technical Specification is not yet available, a corresponding set of requirements has been included in Annex A, which will be removed if the Technical Specification becomes available before the adoption of the EUCS.

Regarding the methodology and conformity assessment methods, they are defined in the annexes of the scheme, while work is ongoing with CEN-CENELEC and with EA on the development of an accreditation guidance for CABs that would provide additional information and a better integration with the ISO/IEC 17065 standard.

POLITICO

9. NECESSARY INFORMATION FOR CERTIFICATION

ARTICLE 54 REFERENCE

Article 54(1). 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, 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.

Before or during the evaluation, the CSP shall submit all the information needed to demonstrate that the implementation of their cloud service meets the service requirements defined in Annex A: (Security Objectives and requirements for Cloud Services) for the targeted evaluation 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 providers are used, records and documents that can provide assurance that the subservice providers satisfy the requirements of the EUCS 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 CS-EL2 and above) and Annex D: (Assessment for level CS-EL1).

For the particular case of evaluation levels CS-EL3 and CS-EL4, the information provided with the application document shall also allow the designated national authority to perform the necessary eligibility checks as defined in the first section of Annex J: (Protection of European data against unlawful access).

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, that is relevant to the cloud service;
- access to additional information that the CAB may request from the CSP for the purpose of the evaluation;

- unrestricted access to personnel within the CSP's 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 certification or assessment of an ICT product, ICT service, or ICT process. 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 activities only when the provided evidence conforms to the requirements for such evidence, the evidence has been analysed following a methodology recognized by the EUCS, 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).

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

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).
- If the CSP uses subservice providers in the provision of the cloud service, the description shall indicate that Complementary Subservice Organization Controls (CSOCs) 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 CSOCs and requirements on these CSOCs assumed in the design of the CSP's controls, and pointers to assurance information where evidence can be found that the subservice provider satisfies the specified requirements on these CSOCs with a level of assurance suitable for the targeted evaluation level. The assurance information referred to in that presentation shall be included in the information provided to the CAB.
- The description shall indicate that Complementary User Entity Controls (CUECs) 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, the CUECs and requirements on these CUECs 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).

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.

RATIONALE

The information to be provided by the CSP is mostly guided by the requirements defined on the security controls in Annex A: (Security Objectives and requirements for Cloud Services). The present chapter only defines the main principles, which grant 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;
- when applicable, 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 requirements on security controls.

10. MARKS AND LABELS

ARTICLE 54 REFERENCE

Article 54(1). 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 expiry, and in association with the certified cloud service: the non-respect of this condition shall be considered as a non-compliance, 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 the EUCS.

RATIONALE

A label and associated mark, established for the European Cybersecurity Certification Framework (ECCF) 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 ECCF, the certification 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 (as a URL provided by ENISA) to the ENISA website (as per Article 50 of the EUCSA) - 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 (<u>basic</u> / <u>substantial</u> / <u>high</u>)	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 EUCS 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 representing the URL provided by ENISA that points to the ENISA's Web site on cybersecurity certification – as per the Article 50 of the EUCSA – and more precisely to the page where the effective status of the certificate of the cloud service and the information regarding its life cycle can be retrieved;
- EUCSA assurance level (with the introduction of a specific colour identifying each level);
- specific EUCS evaluation level;
- the sentence “Certified in the European Union”, together with the flag of the EU.

The label may contain other information, for instance to identify specific cloud service extension profiles that have been included in the certification scope. The introduction of the URL will imply, as defined by Chapter 20 (Disclosure Policy), a procedure for the release of the URL.

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 expiry);
- The assurance level, evaluation level 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 used to ensure that CSPs comply to these requirements.

11. COMPLIANCE MONITORING

ARTICLE 54 REFERENCE

Article 54(1). 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 prevent and where needed to detect the following general cases:

- a non-compliance of the CSP in their application of the rules and obligations related to a certificate issued on their cloud services, including their obligations defined in the EUCSA;
- a non-compliance by a CAB in the conditions under which they implement the processes related to certification and that are not related to the individual cloud service, or to the obligations defined in the EUCSA for CABs;
- a nonconformity of a certified cloud service with the EUCS service requirements, including and not limited to changes in the cloud services and the threat environments.

Monitoring of certified cloud services

The general monitoring of the certified cloud services shall be based on sampling, using generic parameters 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 maintain a multi-annual market surveillance plan outlining their sampling strategy, and implement it every year. Each NCCA should 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 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 audit procedures are defined in Annex G: (Certification Life cycle and continued assurance).

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

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

Monitoring activities shall also include the activities described hereinafter in order to detect non-compliance by CSPs and CABs and nonconformities by certified cloud services.

Non-compliance by a CSP

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 certification of a cloud service, 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 cybersecurity 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 scope⁷;
 - deviation from constraints of the certificate including those of Chapter 12 (Certificate Management)⁸;
 - 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 cybersecurity 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 dependencies⁹, or the list of utilized tools¹⁰.

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 certification 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 conformity assessment 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 certification¹¹;
 - 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 not limited to changes that have an impact on the scope of certification, changes of subservice providers, changes in the supplementary cybersecurity information or in any documentation element that is provided with the certificate.
2. using the following available mechanisms to track the non-respect of the previous obligations:
 - the activities of market surveillance established under Article 58(7), point (a) of the EUCSA, 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;

⁷ e.g., failure to describe some of the underlying capabilities that the service relies on.

⁸ e.g., advertising a certified cloud service after the product certificate has expired.

⁹ e.g., the introduction of new libraries or tools that may adversely impact security

¹⁰ e.g., a change in the tools in the development chain

¹¹ 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 [certificate](#) holders, as to formally check and report the respect of previously stated obligations.

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

Non-compliance by a CAB

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 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), point (b) of the EUCSA;
 - obligations for supervising and enforcing [CAB](#)'s and certificate holder's scheme [compliance](#) as implicitly required by Article 58.7.(a) of the EUCSA;
 - obligations for complaint handling as required by Article 58.7.(f) and Article 63 of the EUCSA;
- 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).

Any [non-compliance](#) with the implementation and operation requirements of the [certification scheme](#) (not related to an individual [cloud service](#)) shall:

1. be avoided where possible through:
 - the audits permitted through Article 58(8), point (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](#) to handle [complaints](#) associated to their [accreditation](#).

Nonconformity of a certified cloud service

The following shall be considered as an alleged [nonconformity](#) of a [certified cloud service](#) with its [certification requirements](#):

- a change in the [certified cloud service](#) itself leading to a change of the [cloud service](#)'s security posture;
- a significant [security incident](#) that has resulted in a data breach or loss of sensitive information, or has otherwise impacted the [certified cloud service](#);
- 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 [nonconformity](#) of a [certified cloud service](#) with its [certification requirements](#) shall be monitored under the following responsibilities:

1. CSPs shall:
 - inform their 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 vulnerabilities that would be relevant to the certified cloud service, either published by or received from end users and security researchers as defined in Article 55(1), point (c) of the EUCSA, 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 significant security incident, including at least those that they or their customers 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 vulnerabilities that would be relevant to their clients' scope of certification;
 - monitor the handling of security incidents reported by CSPs; and
 - report to their NCCA any detected vulnerability affecting the conformity of a certified cloud service to the certification requirements.

Where deemed necessary by the CAB or at the discretion of the NCCA, a series of evaluation activities may be requested to be performed with the support¹² of the CSP as to confirm the impact of a nonconformity.

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

Force majeure

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

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

In addition, the NCCA shall inform ENISA about any extension of certificate validity and provide transparency on reasons and the duration of extension, and ENISA shall make the information available on their website.

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:

¹² Where necessary, support shall imply financial support to described activities.

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 certified cloud service or of its environment.

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

This process benefits of the provisions of the EUCSA:

- market surveillance installed by Article 58(7), point (a);
- obligation on auditing the scheme compliance of CABs and certificate holders mandated by Article 58(8), point (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 to ensure continued compliance as required by Article 54(1), point (j);
- the power of a NCCA – through the power of Article 58(8), point (b) – to launch an investigative audit of either the certificate holder or its 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 vulnerabilities that affect their certified cloud 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. These conditions do not preclude other arrangements, such as a mutualisation of the costs between providers of certified cloud services.

The implementation of compliance monitoring by NCCAs may be the subject of peer review between NCCAs, as defined in Article 59 of the EUCSA. For instance, the sufficiency of the surveillance and monitoring activities are intended to be evaluated in these peer reviews, for instance regarding their sampling strategy and the 5% recommended minimum.

12. CERTIFICATE MANAGEMENT

ARTICLE 54 REFERENCE

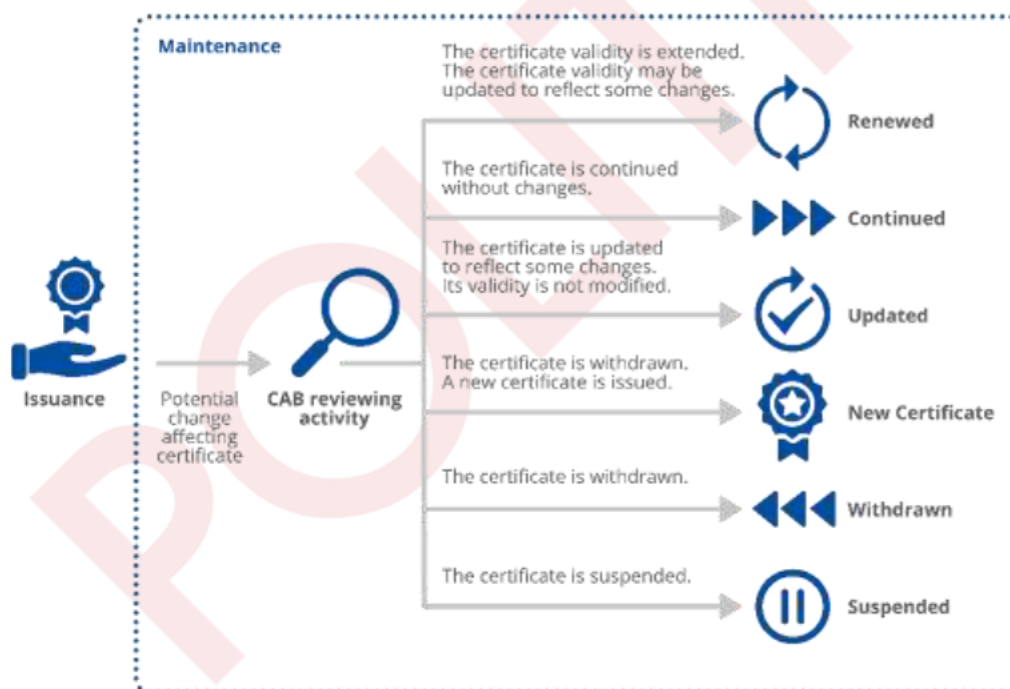
Article 54(1). A European cybersecurity certification scheme shall include at least the following elements:

(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 shall be ISO/IEC 17065 and in particular, its Clause 7.10, where 'changes affecting a certificate' are established.

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 CS-EL2 and above, and Annex D: (Assessment for level CS-EL1) for the requested evaluation 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 evaluation 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 EUCSA.

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 circumstances that require an earlier reassessment, including reasons related to the handling of nonconformities.

Maintenance activities shall be initiated upon the following conditions:

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

Maintenance activities shall be initiated on the request of the certificate holder upon one of the following conditions:

- a surveillance assessment is due to be performed;
- a re-certification 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) of the EUCSA;
- a significant change occurs in the certified cloud service, or in its threat environment, 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 notify the CAB of the NCCA following a complaint, who could in turn trigger maintenance activities.

When the maintenance activities are initiated by the CSP, the request to the CAB shall include a summary of changes and an analysis of their impact, in accordance with Annex G: Certification Life cycle and continued assurance and with Annex F: Scheme Document Content requirements.

In all other cases when the maintenance activities are initiated by any other party (CAB, NCCA, and any party 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 nonconformity or the identified non-compliance and its foreseen impact on the certificate.

Based on the summary of changes and an analysis of their impact provided by the CSP or on the rationale for maintenance provided by another party, and based on the requirements defined in this scheme for surveillance or re-certification assessments, the CAB shall validate which evaluation activities, if any, are deemed necessary before it starts its review and decision, and validate accordingly the scope of and the workload associated to these activities. The CAB shall review the result of the necessary evaluation activities once completed and make a certification decision.

Typical conformity assessment activities are defined in Annex G: Certification Life cycle and continued assurance:

- Surveillance conformity assessment, including a partial re-assessment of the certified cloud service, to be performed at regular intervals, during the validity period of the certificate, as defined in Chapter 19, Certificate validity.
- Recertification conformity assessment, including a full re-assessment of the certified cloud service, to be performed before the expiry date of the certificate.
- Special conformity assessment, following a request from a CSP to consider changes in the certified cloud service, 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 support¹³ 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 evaluation level, or a reduced scope of the certificate to still meet the current evaluation 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 Life cycle 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 expiry date, in the case no maintenance has been requested when a periodic assessment is due, or more generally in the case a maintenance evaluation activity 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, and if the certificate has reached its expiry date, it is then marked 'expired'.

All withdrawn and expired certificates shall be subject to archiving. Archiving shall consist of still providing access to the certificate and associated information, including a clear indication of the reason for its withdrawal, for instance a persistent nonconformity.

¹³ Where necessary, support shall imply financial support to described activities.

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 surveillance assessment or until its expiry date
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 customers without any reduction in the scope of certification or evaluation level	Update the certificate with the new service description and updated audit report and continue the certificate until the next surveillance assessment or until its expiry date
A recertification conformity assessment has been performed and reviewed, and have determined that the cloud service still fulfils the EUCS requirements, possibly with changes that impact the security of customers without any reduction in the scope of certification or evaluation level	Renew the certificate with a new expiry 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 evaluation level	Withdraw the certificate and issue a new certificate with the reduced scope or evaluation level , possibly with a different expiry 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 needed and deemed possible to maintain the certificate at the same evaluation level and scope, though not immediately. Or improper use of the certificate has been identified and has not been addressed 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 [expiry](#) (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 nonconformity with certification requirements, or an identified non-compliance with the accreditation requirements of the CAB, the EUCSA provisions, or the EUCS requirements) has been considered.

One fundamental condition for issuing a certificate for a cloud service is successful evaluation, based on the present scheme. Other conditions stem from relevant provisions of the EUCSA, such as necessary authorisations for CABs 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-compliance 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).

POLITICO

13. NON-COMPLIANCE

ARTICLE 54 REFERENCE

Article 54(1). 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, Compliance Monitoring, defines several categories of non-compliance that may be uncovered through monitoring activities. When instances of such non-compliance are uncovered, the consequences for the various parties, including the CSP, the CAB and its subcontractors, and the NCCA, shall be as follows.

For confirmed deviations or irregularities associated to non-compliance by a CSP to the requirements related to a certificate issued on a cloud service that they provide, 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 EUCSA, 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 evaluation levels CS-EL3 and CS-EL4, 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 EUCS 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 certificate holder of the suspension of the certificate shall mark the beginning of a suspension period of 14 days for certificates at the evaluation levels CS-EL3 and CS-EL4, or 30 days for certificates at the evaluation levels CS-EL1 or CS-EL2. During this period:

- the impact of the non-compliance on the certified cloud service shall be estimated with the necessary support¹⁴ of the CSP;

¹⁴ 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 nonconformity 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 nonconformity and the associated maintenance activities have not been completed, then the certificate shall be withdrawn.

ENISA shall be informed in the due course of the procedure on all outcomes 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 of any extension of a suspension period.

For a confirmed non-compliance in the conditions under which the certification activities have been performed by a CAB 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 CAB or subcontractor that would be in a better technical position to perform these activities, leading to updated evaluation reports;
- the review by the CAB of the updated evaluation 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 evaluation levels CS-EL3 and CS-EL4 or 30 days for certificates at evaluation levels CS-EL1 and CS-EL2, 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 attestation activities shall be supported¹⁵ by the CAB that proved to be non-compliant¹⁶.

¹⁵ Where necessary, support shall imply financial support to described activities.

¹⁶ Or by a subcontractor of the CAB if that subcontractor proved to be non-compliant in breach of its contractual obligations.

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.

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 first simple ruleset is about the handling of non-compliance by a CSP, which needs to be resolved in a short delay.
- The second ruleset is about the case where the non-compliance leads to a nonconformity in the certified cloud service (and its operation).
 - In that ruleset, the CSP has an opportunity to fix the issue without any visible consequence (no suspension, no withdrawal).
 - If the CSP fails to do so timely, then a suspension occurs.
 - There is one exception, when a CSP fails in its continued assurance and maintenance duties, which is considered as non-compliance to the scheme. In that case, 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 normally gets involved (with an opportunity to perform evaluation activities) only if the CSP reports issues as planned.
- The third ruleset is about what happens when a suspension occurs (directly or after failure to act swiftly when a nonconformity 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 may 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 fourth 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 activities may need to be redone, as well as the corresponding review activities, 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 nonconformity is identified in their cloud service during that review, then this nonconformity needs to be handled following the first ruleset (and the second if needed).

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

POLITICO

14. NEW VULNERABILITIES

ARTICLE 54 REFERENCE

Article 54(1). 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. These rules are defined in the present chapter, as well as in the definition of the security controls related to security 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), point (c) of the EUCSA.

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 certified cloud service related to the vulnerability is major¹⁷, 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 moment the CSP learns about the vulnerability and the notification of the CAB shall not exceed five (5) working days for evaluation levels CS-EL1 and CS-EL2, and three (3) working days for evaluation levels CS-EL3 and CS-EL4. Failure to notify the CAB of a vulnerability with potential major impact or to do so within the delays defined above 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 date for the delivery of the full analysis, which shall be within five (5) working days of the

¹⁷ 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.

initial notification, and which may be extended up to ninety (90) days after the CSP became aware of the vulnerability, under justified circumstances and in agreement with the CAB.

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 <https://www.first.org/tlp/>, 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 special 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 for evaluation levels CS-EL1 and CS-EL2, and three (3) working days for evaluation levels CS-EL3 and CS-EL4. When both parties deem necessary or are unable to agree on such decisions, they may inform the NCCA and ask for its advice, and if required for additional delays.
- If a maintenance conformity assessment has been deemed necessary, it shall be performed before lifting a potential suspension of the certificate.

If a vulnerability is reported or discovered during a conformity assessment, the issuance or renewal of a certificate shall not occur as long as the impact of the vulnerability would require the suspension or withdrawal 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 should 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 CSP may apply an embargo period, meaning that the potential vulnerability is not publicly disclosed. During the embargo period, the CSP may disclose the vulnerability to some or all CSCs, including in particular those who operate an EUCS-certified cloud service and may be impacted by the vulnerability.

This embargo 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 CSCs 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, and at the latest when a strategy to correct the issue has been defined by the CSP with the approval of the CAB, the CAB shall disclose information related to the confirmed vulnerability to the NCCA, in accordance with Article 56(8) of the EUCSA.

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), point (h) of the EUCSA share this information with the other NCCAs, which may also decide to further analyse the issue 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 EUCSA. ENISA shall be informed of all 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 certified cloud services.

RATIONALE

The current description has been strongly inspired from the EUCS, 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).

The timelines indicated here are limits, but vulnerabilities are expected to be handled timely. This is why the time for the initial analysis is limited to 90 days (with justification and agreement with CAB), but should normally be under 10 days (5+5).

15. RECORD RETENTION

ARTICLE 54 REFERENCE

Article 54(1). 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 issuing certificates 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, such as ISO/IEC 17025 for CABs performing test activities.

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 consulted on the CSP's premises during the conformity assessment, which shall be retained by the CSP (see Chapter 18, Availability of Information). 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 conformity assessment. In the case that a certificate expires or is withdrawn, the records in storage for this certificate at the time of the expiry or withdrawal shall also be kept for a period of at least five (5) years after the expiry or withdrawal of the certificate.

RATIONALE

The proposal consists in requiring records to be kept for 7 years after a conformity assessment (which roughly corresponds to two certification cycles). In addition, and in order to allow for any possible litigation to conclude, records also need to be kept for 5 years after the expiry or withdrawal of the certificate. So, records should not be kept for more than 12 years, and only in the case of expiry or withdrawal.

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, which needs to include enough information for tracing the documents, e.g., at least a cryptographic digest of the document.

16. RELATED SCHEMES

ARTICLE 54 REFERENCE

Article 54(1). 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 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 scheme¹⁸. In particular, each scheme defines only a single assurance level and some of them do not issue certificates.

Nevertheless, it shall be considered that:

- a certificate issued under these schemes¹⁹ may where necessary²⁰ 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 or assurance report issued under these schemes may be used for certifications under the EUCS scheme whereby the CSP uses the certificate or assurance report as assurance information for subservice providers until its period of validity, if evaluation activities confirms that the subservice provider 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.

¹⁸ 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.

¹⁹ If any, since there are no certificates issued in the context of Germany's C5

²⁰ To satisfy market or regulatory requirements.

Based on the recommendations established by this Chapter, the European Commission and EU Member States may consider to establish a date of two (2) years after the implementing act has been adopted pursuant to Article 49(7) of the [EUCSA](#) for existing schemes to cease producing effect.

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 cybersecurity certification schemes](#), no international schemes have been identified that cover the same [ICT 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 focusing on the cybersecurity of cloud services; these schemes were very different in nature, in some cases not even [issuing](#) any kind of [certificate](#) (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 EUCS for one year, giving the community enough time to develop the required guidance, and also giving NABs, NCCAs and CABs enough time to get the first CABs [accredited](#) and, if needed, [authorised](#). This is covered in greater details in Chapter 25 (Further Recommendations).

17. CERTIFICATE FORMAT

ARTICLE 54 REFERENCE

Article 54(1). 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;

A certificate shall at least include at the following information:

- a unique identifier established by the issuer of the certificate, following a specification to be defined by ENISA to guarantee the unicity across the EU and across certificate versions;
- information related to the certified cloud service and its CSP:
 - name of the cloud service;
 - version for the cloud service;
 - name and contact information of the CSP;
 - link to the website of the CSP to access the Supplementary cybersecurity information for the certified cloud service in accordance with Article 55 of the EUCSA;
- information related to the evaluation and certification of the cloud service:
 - name and contact information of the body or authority that issued the certificate;
 - name of the CAB which performed the audit, when different from the abovementioned body or authority;
 - name of the responsible NCCA;
 - reference to this scheme;
 - reference to the certification report associated with the certificate;
 - assurance level from the EUCSA reached ('basic', 'substantial' or 'high');
 - evaluation level from this scheme (CS-EL1, CS-EL2, CS-EL3 and CS-EL4);
 - where applicable, reference to CSEP(s) to which the cloud service complies;
 - date of issuance and period of validity of the certificate;
- when available, the mark of label associated to the EUCS, as defined by Chapter 10 (Marks and Labels).

Following the registration of the certificate to ENISA for publication on the certification web site, ENISA will provide a unique link for the certificate, possibly associated to a QR-code, that will point to the certificate's page on ENISA's Web site, to be used in all communication about the certificate, possibly in conjunction to the label, when available.

Each certificate shall be signed by the appropriate responsible person of the authority or body and made available to the NCCA and to ENISA with its associated certification report in electronic form and in English language. In case such documents are produced in a language different from English, a courtesy translation shall be provided.

For each certificate, a certification report shall be established by the issuer of the certificate. It shall at least contain the information detailed in Annex F: (Scheme Document Content requirements).

RATIONALE

The content of the EUCS certificates inherits from the content of EUCC certificates, in order to encourage consistency between the certificates issued in the context of the EU Cybersecurity Certification Framework.

ENISA will issue guidance to NCCAs and certificate issuers to guarantee the unicity of certificate identifiers across the EU. In addition, and in conjunction with the framework-level labelling scheme, ENISA may issue unique QR codes and internet links associated to certificates that should allow the CSP, through the documentation associated to a certified cloud service, to facilitate the access by its prospects and customers to the ENISA website where certificates are displayed.

As a certificate cannot encompass all relevant information associated with the certified cloud service, a certification report that contains more detailed information shall be established and published in association with the certificate. A template for the Certification report is included in Annex F: (Scheme Document Content requirements).

POLITICO

18. AVAILABILITY OF INFORMATION

ARTICLE 54 REFERENCE

Article 54(1). 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 as long as the validity of the certificate is maintained through the activities described under Chapter 12 (Certificate Management), and for a period of at least five (5) years after the expiry or withdrawal of the certificate.

Available information shall be updated with the new or revised information related to the activities performed under Chapter 12 (Certificate Management) and to the evolution of the certified cloud service.

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), point (a) of the EUCSA) for seven (7) years after the conformity assessment and up to five (5) years after expiry or withdrawal of the certificate, 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 defined above.

RATIONALE

The period of retention for CSPs shall not be shorter than the retention of records by the CABs, which is of seven (7) years after a conformity assessment and five (5) 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(1). 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 surveillance conformity assessment or to a re-certification conformity assessment at most one (1) year after the previous initial, surveillance, or re-certification conformity assessment.

Under certain conditions, and following the processes defined in Chapter 12 (Certificate Management), including a specific set of evaluation activities, 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 evaluation levels that can be achieved and the associated effort to generate assurance that the EUCS 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 conformity assessments. This limit applies to all evaluation levels, but the nature of the activities to be performed depends on the evaluation level.

20. DISCLOSURE POLICY

ARTICLE 54 REFERENCE

Article 54(1). 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 EUCSA.

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. The issuing CAB shall report any change to the status of a certificate 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. ENISA shall generate for each certificate an internet link that is unique to the certificate, and communicate this link to the CSP and to the CAB who issued the certificate.

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 URL²¹ providing a direct link to the corresponding certificate and related information on the ENISA web site dedicated to EU cybersecurity certification, as to offer a better user experience and to publicise the certificates. ENISA may therefore establish a procedure for the generation of such a URL: the 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 the URL provided by ENISA to the original certificate information

²¹ To be provided in the most appropriate form depending on circumstances, typically a direct link for an online representation or an easily scannable QR-code for physical documentation.

on ENISA's website to allow customers to retrieve 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, then the information published on ENISA's website shall include the starting date and end date 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 archive it to a dedicated section 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 certificates 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 of the EUCSA, a validated link to that information will be made available into the certificate.

ENISA needs to be informed without undue delay of any change to the status 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 EUCSA.

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 or that have been withdrawn will be archived and made available on a different webpage than the valid ones.

21. MUTUAL RECOGNITION

ARTICLE 54 REFERENCE

Article 54(1). 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 MRA 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, review, decision and certification activities 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 F:(Scheme Document Content requirements) 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, where applicable, authorises 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 an assurance level equivalent to assurance level 'high' of the EUCSA 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 assurance levels equivalent to assurance levels 'basic' or 'substantial' of the EUCSA 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:

(105) 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, 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.

With the inclusion of requirements on independence from non-EU laws, it is quite unlikely that any form of mutual recognition can be achieved for evaluation levels CS-EL3 and CS-EL4.

22. PEER ASSESSMENT

ARTICLE 54 REFERENCE

Article 54(1). 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 requires that each authority²² or body issuing certificates at the evaluation levels CS-EL3 and CS-EL4 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 evaluation levels CS-EL3 and CS-EL4 to:

- assess that they work in a harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composition, as offered by Chapter 3 (Purpose of the scheme), including the reuse of a certified secondary cloud service's evaluation results when used for the provision of a primary cloud 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 ECCG²³ 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 CABs that are engaged in activities at assurance level 'high' for the first time or after a long lasting break (more than two years).

²² 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.

²³ 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), point (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. The scope of the assessment shall include the procedure established by of the NCCA for prior approval for each individual certificate.

In the case of Article 56(6), point (b) of the EUCSA, both the CAB issuing the certificates and the NCCA shall be subject to the peer assessment. The scope of the assessment 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, within the peer assessment report, indicating how the peer assessed CAB intends to correct the findings. Where necessary, the ECCG shall 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 views.

The peer assessed CAB and related NCCA shall have the opportunity to address with the ECCG any findings and recommendations identified in the report, before the results of the peer assessment are published by ENISA. Also, the NAB of the peer-assessed CAB shall have the opportunity to address any findings 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 evaluation levels CS-EL3 and CS-EL4 of the EUCS that their certification projects may be subject to the peer assessment installed by this scheme.

The results of the peer assessment shall be made publicly available on the ENISA website dedicated to cybersecurity certification.

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 applies for the supervisory and monitoring body of the NCCA, a peer assessment may be defined for each scheme, with scheme specific objectives defined here for the EUCS in the first part of this Chapter, and associated requirements.

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

It is essential that a programme be established for peer assessment activities, including reassessments, and necessary priorities associated to newcomers to certification, or CABs 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 shall be made publicly available on the ENISA website dedicated to cybersecurity certification, as recommended by Recital 100 of the EUCSA.

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 certificates 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 NAB of the assessed body or authority for their conclusions on the impacts on their authorisation and accreditation.

23. SUPPLEMENTARY INFORMATION

ARTICLE 54 REFERENCE

Article 54(1). 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 publication.

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 up-to-date available at least until the expiry or withdrawal of the corresponding European cybersecurity certificate. Updates shall be made in accordance with the requirements of Chapter 12 (Certificate Management).

In addition, “guidance and recommendations²⁴ to assist end users with the secure configuration, installation, deployment, operation and maintenance of the cloud services”, as defined by Article 55(1), point (a) of the EUCSA, shall be updated as required to reflect the evolution of the cloud service, in accordance with the requirements of Chapter 12 (Certificate Management).

²⁴ 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 of the EUCSA, 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 EUCS. 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 evaluation 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

24.1 EXTENSION PROFILES

The scheme users shall have the ability to extend the EUCS service requirements in the context of a specific use case, defined as a security problem. Such specific requirements shall be defined in an EUCS extension profile (CSEP), following some principles:

- A CSEP shall not remove or weaken any requirement defined in the EUCS.
- A CSEP shall not modify the assessment methodology or the assessment methods defined in the EUCS.
- A CSEP shall follow the processes defined in the EUCS, and shall produce the same deliverables.
- A CSEP shall specify the minimum EUCS evaluation level that it targets.
- A CSEP shall define new service requirements, as long as these requirements do not contradict EUCS service requirements or weaken EUCS service requirements from the evaluation level targeted by the CSEP.
- A CSEP may define a dedicated section in the document templates defined in the EUCS.

In order to be recognized in the context of the EUCS, CSEP certificates shall be published on ENISA's Website, after certification by a CAB notified to issue certificates at the evaluation level targeted by the CSEP.

A CSP shall list in its application document the CSEPs to whose requirements they claim conformity in addition to the core requirements of the EUCS. If this claim is confirmed by the conformity assessment, then the CSP shall include this list of CSEP(s) in the certificate documentation.

Additional details about extension profiles are provided in Annex H: (Extension Profiles).

RATIONALE

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 other conformity assessment schemes, and in particular of other European cybersecurity certification schemes. Some of these conformity assessment schemes may have specific requirements, for instance related to an industry vertical.

In addition, there may be similar additional requirements for cloud services in relation to EU regulations, to requirements from customers, or to other reasons.

In order to simplify the use of certificates issued in the EUCS in other schemes and for specific uses, 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.

Furthermore, in order to guarantee that the quality of the extension profiles is sufficient and that the service requirements that they define do not contradict the principles of the EUCS, it is essential to have a conformity assessment performed on all extension profiles by a CAB with appropriate EUCS competences. This is why a specific certification process has been defined for extension profiles, strongly inspired from the process used in [ISO15408] to certify Common Criteria's Protection Profiles.

24.2 SECURITY OF INFORMATION

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.



Unless otherwise provided for in this scheme and without prejudice to existing national provisions and practices in the Member States on confidentiality, all parties²⁵ 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 GDPR²⁶;
- b) commercially sensitive and confidential information and trade secrets of a natural or legal person, including intellectual property rights, during the certification life cycle of the cloud service and up to the end of the indicated retention time for all certification-related 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;
- d) all information related to investigative, supervisory and monitoring powers of NCCAs and the information related to the accreditation by NABs of the CABs and their subcontractors.

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.

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 ensure the security of information based on the workflows associated with the activities described in the EUCS.

RATIONALE

Security of information is key in cybersecurity related activities. All cybersecurity certification related activities fall into this obligation.

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 evaluation reports, which are associated to the assessment of vulnerabilities, their handling and disclosure, will also contain sensitive information that, when poorly

²⁵ 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.

²⁶ 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).

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 EUCS 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.

24.3 COMPOSITION

Composition is a particular case of certification, in which the cloud service to be certified (then called a primary cloud service in the context of composition) uses a subservice that is itself a cloud service (then called a secondary cloud service) that has been certified in the EUCS. In such a case the primary cloud service relying on the secondary cloud service can expect the assessment of the requirements related to the secondary cloud service to be greatly simplified, because they use the same security framework, and because the rules of the EUCS (including those related to the CABs and to the life cycle of certificates) are trusted.

In order to be eligible for composition, the secondary cloud service shall satisfy specific service requirements on documentation, defined in Annex A: (Security Objectives and requirements for Cloud Services), which allow the assessment of primary 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 shared between the secondary cloud service and the primary cloud service:

- The secondary cloud service provider shall provide a description of the contribution of their cloud service to the EUCS requirement fulfilment of primary cloud services that depend on it, properly justified through references to their own controls²⁷; and
- The secondary cloud service provider shall provide a list of actionable requirements on Complementary Customer Controls (CUECs, based on the EUCS objectives and requirements), to be fulfilled by a primary cloud service that relies on their service in order for that primary cloud service to fulfil the requirements for EUCS certification at the chosen assurance level²⁸.

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

This information shall then be used by the CSP of the primary cloud service in several ways:

- During the design phase, the CSP shall use the information about the secondary cloud service to drive design decisions for its primary cloud service;
- When building documentation for its certification, the description of the secondary cloud service's contribution and of its CUECs shall be used directly by the primary cloud service provider, who will simply need to document its implementation of the CUECs; and
- The CAB shall verify that the certificate of the secondary cloud service is still valid, and that the composition-related information about that secondary cloud service has not been modified and if necessary that a subset has been properly selected, and will focus on verifying that the CUECs defined by secondary cloud service are fulfilled by the primary cloud service.

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

- In order to apply composition, the secondary cloud service shall be certified at an evaluation level equal or greater than the evaluation level targeted by the primary cloud service;

²⁷ This is objective of requirement DOC-05.

²⁸ This is objective of requirement DOC-04.

- In order to apply composition fully, the secondary cloud service shall claim compliance to all the extension profiles that the primary cloud service claims compliance to. If the primary cloud service claims compliance to an extension profile that is not claimed by the secondary cloud service, then this extension profile is excluded from the composition, and a classical process shall be used if necessary to demonstrate that the secondary cloud service satisfies as a subservice the expectations of the primary cloud service relative to the requirements defined in that extension profile;
- The primary cloud service shall add to the requirements to be fulfilled the requirements from the secondary cloud service's CUECs.
- In its description of its contribution of the secondary cloud service to the fulfilment of the EUCS requirements, the primary cloud service shall indicate when the description is the one provided by the secondary cloud service in its documentation.

Finally, note that:

- A primary cloud service may use composition with more than one secondary cloud services;
- Although composition can only be applied to secondary cloud services that have been certified through the EUCS, ENISA will issue with the support of ECCG guidance about a similar approach for secondary cloud services that have been assessed through existing National cybersecurity certification schemes listed in Chapter 16 (Related Schemes), in order to facilitate the transition from National schemes to the EUCS.

RATIONALE

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, processes and services. In the context of the EUCS, the objective is twofold:

- Allow cloud services to be certified along a supply chain.
- Reduce the costs of certifying a cloud service that relies on previously certified products, processes 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 primary cloud services whose operation relies on one or several secondary cloud service providers, and also to the maintenance of the certification for such cloud services, relatively to the maintenance of the certification of their components.

Cloud services are layered systems, in which infrastructure and platform capabilities from a cloud service are often used as a basis for other cloud services. There may also be some dependencies between an application capability offered by a cloud service and another cloud service. These services used by a CSP in the provision of its own cloud service are referred to as subservices, supplied by subservice providers. The general rules for the consideration of such subservice 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 subservice providers and suppliers that are defined in Annex A: (Security Objectives and requirements for Cloud Services).

Composition is a highly desirable mechanism, which greatly simplifies the evaluation of cloud services that depend on other cloud services, which happens to be a very common case. Beyond reducing the complexity (and cost) of the evaluation, composition also reduces the effort to be made by the primary cloud service provider in preparation for the certification of its cloud service. It can therefore be highly beneficial in particular for SMEs who rely on another CSP's infrastructure.

25. FURTHER RECOMMENDATIONS

25.1 TRANSITION TO THE SCHEME

25.1.1 Problem statement

25.1.1.1 EUCSA Reference

Article 57(1) of the [EUCSA](#) – 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) of the [EUCSA](#). 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) of the [EUCSA](#), 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 the European 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. The transition period is therefore split into two successive phases. The first one is devoted to the preparation of the stakeholders, and it ends with the issuance of the first [certificates](#); the second one is devoted to the effective transition from [National schemes](#) to the EUCS, and it ends with the end of the [issuance of certificates](#) according to [National schemes](#).

Prerequisites for scheme operation

Following the adoption of EUCS, in order for relevant bodies in a Member State to start [issuing certificates](#) at the CS-EL1 and CS-EL2 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 EUCS 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 levels CS-EL3 and CS-EL4, the following should also happen:

- the [NCCA](#) establishes how CS-EL3 and CS-EL4 [certificates](#) will be [issued](#) and takes 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 [authorised](#) 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 a period of one (1) year between the adoption of the EUCS and the issuance of the first certificate as being technically acceptable, although a period of eighteen (18) months would be preferable.

Transition period

ENISA may establish associated rules for transitioning to the EUCS. These rules shall be established in cooperation with the ECCG.

For Member States who operate a National cybersecurity certification scheme for which a transition to the EUCS 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 the EUCS scheme, or reuse for composite evaluations and certifications under the EUCS.

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 EUCS 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 period of one (1) year after the issuance of the first certificates to stop issuing certificates following National schemes as being technically acceptable.

25.2 SCHEME MAINTENANCE

25.2.1 Problem statement

25.2.1.1 EUCSA Reference

Article 62(4) of the EUCSA. 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 objectives and associated requirements;
- improve the conformity assessment methodology and associated documents;
- provide guidance to CABs and CSPs about the prerequisites and operation of the EUCS.

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

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.

In addition, some of the elements of the EUCS have been submitted to CEN-CENELEC as a basis for a Technical Specification, and eventually for a European Standard, and further elements may be submitted to other European Standards-defining Organisations (ESOs). Whenever such Technical Specifications or European Standards, they shall be considered in the development of future releases of the EUCS, and the expert groups in charge of the maintenance of the EUCS shall establish a liaison with the ESOs for those elements of the scheme that are maintained by these ESOs.

POLITICO

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
[ISO22123-1]	ISO/IEC 22123-1:2014, 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 27001:2022, 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) v3.2, 2022.
Available from: <https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/>
- [ZekerOnline] Keurmerk Zeker-Online – Framework of Standards, v3.1, 2016.
Available from: <https://zeker-online.nl/wp-content/uploads/2018/03/framework-of-standards-zeker-online-english-version-3.1-legal-infra-and-generic-and-specific-accounting-application.pdf>
- [ZekerOnlineAudit] Keurmerk Zeker-Online – Audit Protocol, v3.2, February 2017.
Available from: https://zeker-online.nl/wp-content/uploads/2018/03/audit-protocol-3.1-en_final.pdf

[OWASP CA]

Open Web Application Security Project (OWASP) Foundation. Component Analysis.
Available from: https://owasp.org/www-community/Component_Analysis

POLITICO

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

POLITICO

A.1 INTRODUCTION

The EUCS service requirements shall include:

- the requirements defined in the present Annex in sections A.3 to A.22;
- the requirements defined in Annex J: (Protection of European data against unlawful access), section J.2;
- the requirements defined in Annex H: (Extension Profiles), section H.3, which only apply to the certification of EUCS extension profiles.

EDITOR'S NOTE:

The content of sections A.2 to A.22 of the present annex has been submitted to CEN-CENELEC JTCS13's WG2 for adoption as a Technical Specification. The discussions are under way, and if a Technical Specification is adopted that matches the expectations of the EUCS, the requirements in this Annex will be replaced by a reference to the adopted Technical Specification.

In addition, most requirements include indications for the required guidance for this requirement, which are present for reference and will most likely not be included in the final version of the requirements.

Finally, the requirements included below are NOT the latest version of the requirements discussed in JTC13, but the version that was available at the end of 2022.

A.2 PRINCIPLES

The requirements on security controls are an essential component of the EUCS, as they define the technical objectives and requirements that CSPs need to fulfil in order to get a cloud service certified. These requirements have been defined based on the following principles.

Abstraction level

Because this annex is intended to also be an annex to the implementing act for the EUCS, 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 should provide the EUCS 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" (see Annex K: Terminology, for a definition of this term).

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 evaluation level.

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 and evaluation levels

The requirements defined in the present Annex are labelled Basic, Substantial or High, and they are defined relatively to the assurance levels defined in the EUCSA. Typically, the requirements corresponding to an objective are organized as follows:

- Basic requirements define a baseline, often with limited details or constraints. These requirements apply to evaluation level CS-EL1.
- Substantial requirements add to that baseline further details and constraints, although some Basic requirements are left unchanged. Sometimes, there are a few specific Substantial requirements. These requirements apply to evaluation level CS-EL2.
- High requirements add further constraints, both by refining some requirements and by adding specific ones. Some are also related to continuous monitoring, or to additional testing and review requirements, contributing to an increase in the depth of the audit. These requirements apply to evaluation levels CS-EL3 and CS-EL4.

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;
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 levels CS-EL3 and CS-EL4, remains a mid- or long-term objective, and the introduction of automated monitoring requirements in at least some areas is a first step in that direction, which can be met with the technology available today.

ENISA may develop, in collaboration with the ECCG, further guidance about suitable implementations of monitoring.

A.3 ORGANISATION OF INFORMATION SECURITY

PLAN, IMPLEMENT, MAINTAIN AND CONTINUOUSLY IMPROVE THE INFORMATION SECURITY FRAMEWORK WITHIN THE ORGANISATION.

A.3.1 OIS-01 Information Security Management System

A.3.1.1 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.

A.3.1.2 Requirements

Basic	The CSP shall document the scope of the <u>cloud service</u> that is under the <u>CSP's</u> control and the boundaries.	OIS-01.1B
	The CSP shall have an <u>information security management system (ISMS)</u> , covering at least the operational units, locations, people and <u>processes</u> for providing the <u>cloud service</u> .	OIS-01.2B
	The CSP shall provide documented information about the <u>ISMS</u> as applied to the cloud service, covering what is applicable to the <u>cloud service</u> regarding: <ul style="list-style-type: none"> • Scope and boundaries of the <u>ISMS</u>; • The context of the <u>CSP</u>; • Description of how the <u>cloud service</u> is covered by the activities in the <u>ISMS</u>; • How the security of the <u>cloud service</u> is <u>maintained</u> and improved. 	OIS-01.3B
Substantial	The CSP shall document the scope of the <u>cloud service</u> that is under the <u>CSP's</u> control and the boundaries.	OIS-01.1S
	The CSP shall have an <u>information security management system (ISMS)</u> , covering at least the operational units, locations, people and <u>processes</u> for providing the <u>cloud service</u> .	OIS-01.2S
	The CSP shall <u>provide</u> documented information about the <u>ISMS</u> as applied to the <u>cloud service</u> , covering what is applicable <u>to the cloud service</u> regarding: <ul style="list-style-type: none"> • Scope and boundaries of the <u>ISMS</u>; • The context of the <u>CSP</u>; • Description of how the <u>cloud service</u> is covered by the activities in the <u>ISMS</u>; • How the security of the <u>cloud service</u> is <u>maintained</u> and improved. 	OIS-01.3S
High	The CSP shall document the scope of the <u>cloud service</u> that is under the <u>CSP's</u> control and the boundaries.	OIS-01.1H
	The CSP shall have an <u>information security management system (ISMS)</u> , covering at least the operational units, locations, people and <u>processes</u> for providing the <u>cloud service</u> .	OIS-01.2H
	The CSP shall <u>provide</u> documented information about the <u>ISMS</u> as applied to the <u>cloud service</u> , covering what is applicable <u>to the cloud service</u> regarding: <ul style="list-style-type: none"> • Scope and boundaries of the <u>ISMS</u>; • The context of the <u>CSP</u>; • Description of how the <u>cloud service</u> is covered by the activities in the <u>ISMS</u>; • How the security of the <u>cloud service</u> is <u>maintained</u> and improved. 	OIS-01.3H

A.3.1.3 Guidance requirements

- Define the notion of accredited CAB, including a reference to Regulation 765/2008.
- Reuse of evidence would be expected from an ISO/IEC 27001 certification

A.3.2 OIS-02 Segregation of Duties

A.3.2.1 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 CSC data processed, stored or transmitted in the cloud service.

A.3.2.2 Requirements

Basic	<p>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 CSC covering 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:</p> <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. <p>The CSP shall implement the mitigating measures defined in the risk assessment, prioritising separation of duties.</p> <p>If implementation of the mitigating measures is impossible for organisational or technical reasons, 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.</p>	<p>OIS-02.1B</p> <p>OIS-02.2B</p> <p>OIS-02.3B</p>
Substantial	<p>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, covering 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:</p> <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. <p>The CSP shall implement the mitigating measures defined in the risk assessment, prioritising separation of duties.</p> <p>If implementation of the mitigating measures is impossible for organisational or technical reasons, 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.</p> <p>The CSP shall</p> <ul style="list-style-type: none"> • introduce and maintain an inventory of conflicting roles; • enforces the segregation of duties during the assignment or modification of roles as part of the role management process. 	<p>OIS-02.1S</p> <p>OIS-02.2S</p> <p>OIS-02.3S</p> <p>OIS-02.4S</p>
High	<p>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, covering 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:</p> <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. <p>The CSP shall implement the mitigating measures defined in the risk assessment, prioritising separation of duties.</p> <p>If implementation of the mitigating measures is impossible for organisational or technical reasons, 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.</p> <p>The CSP shall</p> <ul style="list-style-type: none"> • introduce and maintain an inventory of conflicting roles; • enforce the segregation of duties during the assignment or modification of roles as part of the role management process. <p>The CSP shall monitor the assignment of responsibilities and tasks to ensure that measures related to segregation of duties are enforced.</p>	<p>OIS-02.1H</p> <p>OIS-02.2H</p> <p>OIS-02.3H</p> <p>OIS-02.4H</p> <p>OIS-02.5H</p>

A.3.2.3 Guidance requirements

- Include guidance on how the risk assessment should cover administrative user rights and whether the user is authorised to modify or delete the logs or log analysis of their actions

A.3.3 OIS-03 Contact with Authorities and Interest Groups

A.3.3.1 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).

A.3.3.2 Requirements

Basic	The CSP shall stay informed about current <u>threats</u> and <u>vulnerabilities</u> related to the <u>cloud service</u> .	OIS-03.1B
Substantial	The CSP shall maintain contacts with the relevant information security-related authorities and appropriate industry technical groups to stay informed about current <u>threats</u> and <u>vulnerabilities</u> related to the <u>cloud service</u> .	OIS-03.1S
High	The CSP shall maintain contacts with the relevant information security-related authorities and appropriate industry technical groups to stay informed about current <u>threats</u> and <u>vulnerabilities</u> related to the <u>cloud service</u> .	OIS-03.1H

A.3.3.3 Guidance requirements

- The CSP should obtain threat intelligence from an external source and/or collate threat information from its own sources (High).
- Note that the EUCS also requires regular contacts with the CAB and NCCA about vulnerabilities, as part of compliance monitoring

A.3.4 OIS-04 Information Security in Project Management

A.3.4.1 Objective

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

A.3.4.2 Requirements

Basic	The CSP shall incorporate the consideration of information security into the project management activities throughout the project lifecycle of all projects that may affect the provision of the <u>cloud service</u> , regardless of the nature of the project.	OIS-04.1B
Substantial	The CSP shall perform a <u>risk assessment</u> according to RM-01 and if necessary proceed with <u>risk treatment</u> , to assess and treat the risks on all projects that may affect the provision of the <u>cloud service</u> , regardless of the nature of the project.	OIS-04.1S
High	The CSP shall perform a <u>risk assessment</u> according to RM-01 and if necessary proceed with <u>risk treatment</u> , to assess and treat the risks on all projects that may affect the provision of the <u>cloud service</u> , regardless of the nature of the project.	OIS-04.1H

A.3.4.3 *Guidance requirements*

- The risk assessment may be trivial on projects with no or limited effect on the provision of the cloud service.
- For projects with no effect, the risk analysis only needs to show this “non-effect”

POLITICO

A.4 INFORMATION SECURITY POLICIES

PROVIDE A GLOBAL INFORMATION SECURITY POLICY, DERIVED INTO POLICIES AND PROCEDURES REGARDING SECURITY REQUIREMENTS AND TO SUPPORT BUSINESS REQUIREMENTS.

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>

A.4.1 ISP-01 Global Information Security Policy

A.4.1.1 Objective

The top management of the CSP has adopted an information security policy and communicated it to internal and external employees as well as CSCs.

A.4.1.2 Requirements

Basic	<p>The CSP shall <u>document an information security policy</u> covering at least the following aspects: ISP-01.1B</p> <ul style="list-style-type: none"> the importance of information security, based on the requirements of CSCs 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 cloud service provided; the security objectives and the desired security level, based on the business goals and tasks of the CSP; 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 established security objectives. <p>The CSP's top management shall <u>approve and endorse the global information security policy</u>. ISP-01.2B</p> <p>The CSP shall <u>communicate and make available the global information security policy</u> to internal and external employees and to CSCs. ISP-01.3B</p>
Substantial	<p>The CSP shall <u>document an information security policy</u> covering at least the following aspects: ISP-01.1S</p> <ul style="list-style-type: none"> the importance of information security, based on the requirements of CSCs 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 cloud service provided; the security objectives and the desired security level, based on the business goals and tasks of the CSP; 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 established security objectives. <p>The CSP's top management shall <u>approve and endorse the global information security policy</u>. ISP-01.2S</p> <p>The CSP shall <u>review the global information security policy on a regular basis and at least following any significant organisational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management</u>. ISP-01.4S</p>

	The CSP shall communicate and make available the global information security policy to internal and external employees and to CSCs.	ISP-01.3S
High	<p>The CSP shall document an information security policy covering at least the following aspects:</p> <ul style="list-style-type: none"> the importance of information security, based on the requirements of CSCs 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 cloud service provided; the security objectives and the desired security level, based on the business goals and tasks of the CSP; 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 established security objectives. <p>The CSP's top management shall approve and endorse the global information security policy.</p> <p>The CSP shall review the global information security policy at least annually and at least following any significant organisational change susceptible to affect the principles defined in the policy, including the approval and endorsement by top management.</p> <p>The CSP shall communicate and make available the global information security policy to internal and external employees and to CSCs.</p>	<p>ISP-01.1H</p> <p>ISP-01.2H</p> <p>ISP-01.4H</p> <p>ISP-01.3H</p>

A.4.1.3 Guidance requirements

- Position the global policy as defining the principles on which the detailed security policies and procedures are built
- Recall that top management cannot delegate approval here.

A.4.2 ISP-02 Security Policies and Procedures

A.4.2.1 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 CSP in an appropriate manner.

A.4.2.2 Requirements

Basic	<p>The CSP shall derive topic-specific policies and procedures from the information security policy for all relevant subject matters applicable to the cloud service, and document them according to a uniform structure, including at least the following aspects:</p> <ul style="list-style-type: none"> Objectives; Scope; Roles and responsibilities within the organisation; Roles and dependencies on other organisations (especially CSCs and subservice providers); Steps for the execution of the security strategy; and Applicable legal and regulatory requirements <p>The CSP shall communicate and make available the topic-specific policies and procedures to all internal and external employees.</p> <p>The CSP's top management shall approve the topic-specific security policies and procedures or delegate this responsibility to authorized bodies</p> <p>The CSP's subject matter experts shall review the topic-specific policies and procedures for adequacy at least annually, when the global information security policy is modified, and when major changes may affect the security of the cloud service</p> <p>After a modification of topic-specific procedures and policies they shall be approved before they become effective, and then communicated and made available to internal and external employees</p>	<p>ISP-02.1B</p> <p>ISP-02.2B</p> <p>ISP-02.3B</p> <p>ISP-02.4B</p> <p>ISP-02.5B</p>
Substantial	<p>The CSP shall derive topic-specific 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:</p> <ul style="list-style-type: none"> Objectives; 	ISP-02.1S

	<ul style="list-style-type: none"> • Scope; • Roles and responsibilities within the organisation, including personnel competence requirements and the establishment of substitution rules; • Roles and dependencies on other organisations (especially CSCs and subservice providers); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements. <p>The CSP shall communicate and make available the topic-specific policies and procedures to all internal and external employees.</p> <p>The CSP's top management shall approve the topic-specific security policies and procedures or delegate this responsibility to authorized bodies.</p> <p>In case of a delegation, the authorized bodies shall report at least annually to the top management on the topic-specific security policies and their implementation.</p> <p>The CSP's subject matter experts shall review the topic-specific policies and procedures for adequacy at least annually, when the global information security policy is modified, and when major changes may affect the security of the cloud service.</p> <p>After a modification of topic-specific procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.</p>	<p>ISP-02.2S</p> <p>ISP-02.3S</p> <p>ISP-02.6S</p> <p>ISP-02.4S</p> <p>ISP-02.5S</p>
High	<p>The CSP shall derive topic-specific 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:</p> <ul style="list-style-type: none"> • Objectives; • Scope; • Roles and responsibilities within the organisation, including personnel competence requirements and the establishment of substitution rules; • Roles and dependencies on other organisations (especially CSCs and subservice providers); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements. <p>The CSP shall communicate and make available the topic-specific policies and procedures to all internal and external employees.</p> <p>The CSP's top management shall approve the topic-specific security policies and procedures or delegate this responsibility to authorized bodies.</p> <p>In case of a delegation, the authorized bodies shall report at least annually to the top management on the topic-specific security policies and their implementation.</p> <p>The CSP's subject matter experts shall review the topic-specific policies and procedures for adequacy at least annually, when the global information security policy is modified, and when major changes may affect the security of the cloud service.</p> <p>After a modification of topic-specific policies and procedures, they shall be approved before they become effective, and then communicated and made available to internal and external employees.</p>	<p>ISP-02.1S</p> <p>ISP-02.2S</p> <p>ISP-02.3S</p> <p>ISP-02.6S</p> <p>ISP-02.4S</p> <p>ISP-02.5S</p>

A.4.2.3 Guidance requirements

- Recall good delegation practices and what it entails.
 - Describe what the "according to ISP-02" qualifier means in other requirements
- a) In particular, explain why we use "define" instead of document and communicate in most places

A.4.3 ISP-03 Exceptions

A.4.3.1 Objective

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

A.4.3.2 Requirements

Basic	<p>The CSP shall maintain a list of exceptions to the security policies and procedures, including associated controls.</p> <p>The exceptions shall be limited in time.</p>	<p>ISP-03.1B</p> <p>ISP-03.2B</p>
-------	--	-----------------------------------

	The exceptions shall be documented.	ISP-03.3B
	The exceptions shall not lead to a <u>nonconformity</u> to any of the <u>certification requirements</u> of a <u>certified cloud service</u> .	ISP-03.4B
	The list of exceptions shall be <u>reviewed</u> at least annually.	ISP-03.5B
Substantial	The <u>CSP</u> shall <u>maintain</u> a list of exceptions to the security <u>policies</u> and <u>procedures</u> , including associated <u>controls</u> .	ISP-03.1S
	The exceptions shall be limited in time.	ISP-03.2S
	The exceptions shall be documented	ISP-03.3S
	The exceptions shall not lead to a <u>nonconformity</u> to any of the <u>certification requirements</u> of a <u>certified cloud service</u> .	ISP-03.4S
	The exceptions shall be subjected to the RM-01 <u>risk management</u> process, including <u>approval</u> of these <u>exceptions</u> and acceptance of the associated <u>risks</u> by the <u>risk owners</u>.	ISP-03.6S
	The list of exceptions shall be <u>reviewed</u> at least annually.	ISP-03.5S
	The <u>approval</u> of exceptions shall be reiterated at least annually, even if the list has not been modified.	ISP-03.7S
High	The <u>CSP</u> shall <u>maintain</u> a list of exceptions to the security <u>policies</u> and <u>procedures</u> , including associated <u>controls</u> .	ISP-03.1H
	The exceptions shall be limited in time.	ISP-03.2H
	The exceptions shall be documented.	ISP-03.3H
	The exceptions shall not lead to a <u>nonconformity</u> to any of the <u>certification requirements</u> of a <u>certified cloud service</u> .	ISP-03.4H
	The exceptions shall be subjected to the RM-01 <u>risk management</u> process, including <u>approval</u> of these <u>exceptions</u> and acceptance of the associated <u>risks</u> by the <u>risk owners</u> .	ISP-03.6H
	The exceptions to the <u>security policy</u> or <u>procedure</u> shall be <u>approved</u> by the <u>top management</u> who <u>approved</u> the <u>security policy</u> or <u>procedure</u>.	ISP-03.8H
	The exceptions to a topic-specific <u>security policy</u> or <u>procedure</u> shall be <u>approved</u> by the appropriate level of management who <u>approved</u> the topic-specific <u>security policy</u> or <u>procedure</u>.	ISP-03.9H
	The list of exceptions shall be <u>reviewed</u> at least annually.	ISP-03.5H
	<u>The approval</u> of exceptions shall be reiterated at least annually, even if the list has not been modified.	ISP-03.7H
	The list of exceptions shall be automatically monitored to ensure that the validity of approved exceptions has not expired and that all <u>reviews</u> and <u>approvals</u> are up-to-date.	ISP-03.10H

A.4.3.3 Guidance requirements

- Define clearly the notion of appropriate level of management.

A.5 RISK MANAGEMENT

PROVIDE A RISK MANAGEMENT FRAMEWORK, TO MANAGE THE RISKS ASSOCIATED TO THE CSP'S ACTIVITIES, FROM IDENTIFICATION TO TREATMENT.

Term	Definition
risk	<p>effect of uncertainty on objectives</p> <p>Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.</p> <p>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).</p> <p>Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.</p> <p>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.</p> <p>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.</p> <p>[SOURCE: From ISO Guide 73:1.1]</p>
risk owner	<p>person or entity with the accountability and authority to manage a risk</p> <p>[SOURCE: From ISO Guide 73:3.5.1.5]</p>
risk management	<p>coordinated activities to direct and control an organization with regard to risk</p> <p>[SOURCE: From ISO Guide 73:2.1]</p>
risk assessment	<p>overall process of risk identification, risk analysis and risk evaluation</p> <p>[SOURCE: From ISO Guide 73:3.4.1]</p>
risk identification	<p>process of finding, recognizing and describing risks</p> <p>Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.</p> <p>Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.</p> <p>[SOURCE: From ISO Guide 73:3.5.1]</p>
risk analysis	<p>process to comprehend the nature of risk and to determine the level of risk</p> <p>Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.</p> <p>Note 2 to entry: Risk analysis includes risk estimation.</p> <p>[SOURCE: From ISO Guide 73:3.6.1]</p>
risk evaluation	<p>process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable</p> <p>Note 1 to entry: Risk evaluation assists in the decision about risk treatment.</p> <p>[SOURCE: From ISO Guide 73:3.7.1]</p>
risk treatment	<p>process to modify risk (1.1)</p> <p>Note 1 to entry: Risk treatment can involve:</p> <ul style="list-style-type: none"> • avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • taking or increasing risk in order to pursue an opportunity; • removing the risk source; • changing the likelihood; • changing the consequences; • sharing the risk with another party or parties [including contracts and risk financing]; and

Term	Definition
	<ul style="list-style-type: none"> retaining the risk by informed decision. <p>Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".</p> <p>Note 3 to entry: Risk treatment can create new risks or modify existing risks.</p> <p>[SOURCE: From ISO Guide 73:3.8.1]</p>
residual risk	<p>risk remaining after risk treatment</p> <p>Note 1 to entry: Residual risk can contain unidentified risk.</p> <p>Note 2 to entry: Residual risk can also be known as "retained risk".</p> <p>[SOURCE: From ISO Guide 73:3.8.1.6]</p>

A.5.1 RM-01 Risk Management Policy

A.5.1.1 Objective

Risk management policies and procedures are documented and communicated to relevant parties.

A.5.1.2 Requirements

Basic	<p>The CSP shall define policies and procedures in accordance with ISP-02 for the following aspects:</p> <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 cloud service and assigning risk owners; Analysis of the likelihood and consequence and determination of the level of risk; Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of risk treatment; Treatment of risks, including approval of authorisation and acceptance of residual risk by risk owners; Ensuring that the risk assessment activities provide consistent, valid and comparable results; and Retaining documented information of the risk assessment activities. 	RM-01.1B
Substantial	<p>The CSP shall define policies and procedures in accordance with ISP-02 and using a documented risk analysis method that guarantees reproducibility and comparability, for the following aspects:</p> <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 cloud service and assigning risk owners; Analysis of the likelihood and consequence and determination of the level of risk; Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of risk treatment; Treatment of risks, including approval of authorisation and acceptance of residual risk by risk owners; Ensuring that the risk assessment activities provide consistent, valid and comparable results; Retaining documented information of the risk assessment activities. 	RM-01.1S
High	<p>The CSP shall define policies and procedures in accordance with ISP-02 and using a documented risk analysis method that guarantees reproducibility and comparability, for the following aspects:</p> <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 cloud service and assigning risk owners; Analysis of the likelihood and consequence and determination of the level of risk; Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of risk treatment; Treatment of risks, including approval of authorisation and acceptance of residual risk by risk owners; and 	RM-01.1H

- Ensuring that the risk assessment activities provide consistent, valid and comparable results;
- Retaining documented information of the risk assessment activities.

A.5.1.3 Guidance requirements

- External references are needed, in particular ISO27005 for the terminology and ISO31000 for the methodology.

A.5.2 RM-02 Risk Assessment Implementation

A.5.2.1 Objective

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

A.5.2.2 Requirements

Basic	The CSP shall <u>implement the policies and procedures</u> covering <u>risk assessment</u> on the entire cloud service.	RM-02.1B
	The CSP shall <u>make the results of the risk assessment</u> available to relevant internal parties.	RM-02.2B
	Information, specific for their purposes, shall be made available to relevant external parties.	RM-02.3B
	The CSP shall <u>review the risk assessment</u> at least annually, and after each major change that may affect the security of the <u>cloud service</u> .	RM-02.4B
	The CSP shall <u>monitor the evolution of the risk factors</u> and <u>review the risk assessment</u> accordingly.	RM-02.5B
Substantial	The CSP shall <u>implement the policies and procedures</u> covering <u>risk assessment</u> on the entire cloud service.	RM-02.1S
	The CSP shall <u>make the results of the risk assessment</u> available to relevant internal parties.	RM-02.2S
	Information, specific for their purposes, shall be made available to relevant external parties.	RM-02.3S
	The CSP shall <u>review the risk assessment</u> at least annually, and after each major change that may affect the security of the cloud service.	RM-02.4S
	The CSP shall <u>monitor the evolution of the risk factors</u> and <u>review the risk assessment</u> accordingly.	RM-02.5S
High	The CSP shall <u>implement the policies and procedures</u> covering <u>risk assessment</u> on the entire cloud service.	RM-02.1H
	The CSP shall <u>make the results of the risk assessment</u> available to relevant parties.	RM-02.2H
	Information, specific for their purposes, shall be made available to relevant external parties.	RM-02.3H
	The CSP shall <u>review the risk assessment</u> at least annually, and after each major change that may affect the security of the <u>cloud service</u> .	RM-02.4H
	The CSP shall <u>monitor the evolution of the risk factors</u> and <u>review the risk assessment</u> accordingly.	RM-02.5H

A.5.2.3 Guidance requirements

- Define the notion of relevant parties (most likely internal)
- The scope of risk identification should include at least the aspects below, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider:
 - Processing, storage or transmission of data of cloud customers with different protection needs;
 - Occurrence of weak points and malfunctions in technical protective measures for separating shared resources;
 - Occurrence of weak points and malfunctions in the integration at system level of technical protective measures;
 - Attacks via access points, including interfaces accessible from public networks (in particular administrative interfaces);

- Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and
- Dependencies on subservice organisations.
- For higher assurance levels, specific technical risks should be considered, including:
 - The risks of failure of the mechanisms of partitioning technical infrastructure resources (memory, calculation, storage, network) that are shared between clients; and
 - The risks linked to the incomplete or non-secure erasing of data stored in the memory areas or of storage shared between clients, in particular during reallocations of memory and storage areas.

A.5.3 RM-03 Risk Treatment Implementation

A.5.3.1 Objective

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

A.5.3.2 Requirements

Basic	The CSP shall prioritize the <u>risk treatment</u> according to the level of <u>information security risk</u> related to the cloud service.	RM-03.1B
	The CSP shall <u>document</u> and <u>implement</u> a <u>risk treatment plan</u> based on the <u>risk assessment</u>	RM-03.2B
	The <u>risk treatment plan</u> shall reduce the <u>risk level</u> to a <u>residual risk</u> acceptable to the risk owners.	RM-03.3B
	The CSP shall make the <u>risk treatment plan</u> available to relevant internal parties, including appropriately summarised and abstracted versions.	RM-03.4B
	The CSP shall determine if relevant external parties shall receive information, specific for their purposes, about the <u>risk treatment plan</u> and to what extent.	RM-03.5B
	If the CSP shares risks with the CSC, the shared risks shall be associated to <u>Complementary User Entity Controls (CUECs)</u> and described in the user documentation.	RM-03.6B
	The CSP shall review the <u>risk treatment plan</u> every time the <u>risk assessment</u> is modified.	
Substantial	The CSP shall prioritize the <u>risk treatment</u> according to the level of <u>information security risk</u> related to the cloud service.	RM-03.1S
	The CSP shall <u>document</u> and <u>implement</u> a <u>risk treatment plan</u> of the chosen <u>risk treatment options</u> based on the <u>risk assessment</u> .	RM-03.2S
	The <u>risk treatment plan</u> shall reduce the <u>risk level</u> to a <u>residual risk</u> acceptable to the risk owners	RM-03.3S
	The <u>risk owners</u> shall formally accept the <u>risk treatment plan</u> .	RM-03.8S
	The CSP shall make the <u>risk treatment plan</u> available to relevant internal parties, including summarised and abstracted versions.	RM-03.4S
	The CSP shall determine if relevant external parties shall receive information, specific for their purposes, about the <u>risk treatment plan</u> and to what extent.	RM-03.5S
	If the CSP shares risks with the CSC, the shared risks shall be associated to <u>Complementary User Entity Controls (CUECs)</u> and described in the user documentation.	RM-03.6S
	The CSP shall review the <u>risk treatment plan</u> every time the <u>risk assessment</u> is modified.	RM-03.7S
	The <u>risk owners</u> shall review for adequacy the analysis, evaluation and treatment of risks including the approval of actions and acceptance of residual risks, after each modification of the <u>risk assessment</u> and <u>treatment plans</u> .	RM-03.9S
High	The CSP shall prioritize the <u>risk treatment</u> according to the level of <u>information security risk</u> related to the cloud service.	RM-03.1H
	The CSP shall <u>document</u> and <u>implement</u> a <u>risk treatment plan</u> of the chosen <u>risk treatment options</u> based on the <u>risk assessment</u> .	RM-03.2H
	The <u>risk treatment plan</u> shall reduce the <u>risk level</u> to a <u>residual risk</u> acceptable to the risk owners.	RM-03.3H

The risk owners shall formally accept the risk treatment plan.	RM-03.8H
The CSP shall make the risk treatment plan available to relevant parties, with appropriately summarised and abstracted versions.	RM-03.4H
The CSP shall determine if relevant external parties shall receive information, specific for their purposes, about the risk treatment plan and to what extent.	RM-03.5H
If the CSP shares risks with the CSC, the shared risks shall be associated to Complementary User Entity Controls (CUECs) and described in the user documentation.	RM-03.6H
The CSP shall review the risk treatment plan every time the risk assessment is modified.	RM-03.7H
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 modification of the risk assessment and treatment plans.	RM-03.9S

A.5.3.3 Guidance requirements

- The notion of sharing with external parties should be explained as depending mostly on a “need-to-know” basis.
- Sharing risks with customers should always be explicit, and associated with clear expectations, typically expressed as CUECs, and included in the documentation (cf. DOC-01).

A.6 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.

Term	Definition
personnel	persons doing work under the CSP's direction Note 1 to entry: The concept of personnel includes the CSP's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.
employee	a person under employment contract with the CSP to whom human resource management controls apply

A.6.1 HR-01 Human Resource Policies

A.6.1.1 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.

A.6.1.2 Requirements

Basic	The CSP shall classify <u>information security-sensitive</u> positions according to their level of <u>risk</u> , including positions related to IT administration and to the provisioning of the cloud service in the <u>production environment</u> , and all positions with access to <u>CSC data</u> or <u>system components</u>	HR-01.1B
	The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement by <u>personnel</u> to act ethically in their professional duties.	HR-01.2B
	The CSP shall define and implement a <u>policy</u> that describes actions to take in the event of violations of policies and procedures or applicable legal and regulatory requirements including at least the following aspects:	HR-01.3B
	<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 	
	If disciplinary measures are defined in this <u>policy</u> , then the <u>personnel</u> of the <u>CSP</u> shall be informed about possible disciplinary measures.	HR-01.4B
Substantial	The <u>policy</u> shall state that the use of these disciplinary measures shall be appropriately <u>documented</u> .	HR-01.5B
	The CSP shall classify <u>information security-sensitive</u> positions according to their level of <u>risk</u> , including positions related to IT administration and to the provisioning of the cloud service in the <u>production environment</u> , and all positions with access to <u>CSC data</u> or <u>system components</u> .	HR-01.1S
	The CSP shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement by <u>personnel</u> to act ethically in their professional duties.	HR-01.2S
	The CSP shall define and implement a <u>policy</u> that describes actions to take in the event of violations of policies and procedures or applicable legal and regulatory requirements, including at least the following aspects:	HR-01.3S
	<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 	

	If disciplinary measures are defined in this policy, then the <u>personnel</u> of the <u>CSP</u> shall be informed about possible disciplinary measures.	HR-01.4S
	The <u>policy</u> shall state that the use of these disciplinary measures shall be appropriately documented.	HR-01.5S
High	The <u>CSP</u> shall classify information security-sensitive positions according to their level of <u>risk</u> , including positions related to IT administration and to the provisioning of the <u>cloud service</u> in the <u>production environment</u> , and all positions with access to <u>CSC data</u> or <u>system components</u> .	HR-01.1H
	The <u>CSP</u> shall include in its employment contracts or on a dedicated code of conduct or ethics an overarching agreement by <u>personnel</u> to act ethically in their professional duties.	HR-01.2H
	The <u>CSP</u> shall define and implement a <u>policy</u> that describes actions to take in the event of violations of <u>policies</u> and <u>procedures</u> or applicable legal and regulatory <u>requirements</u> , including at least the following aspects:	HR-01.3H
	<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 	
	If disciplinary measures are defined in this policy, then the <u>personnel</u> of the <u>CSP</u> shall be informed about possible disciplinary measures	HR-01.4H
	The <u>policy</u> shall state that the use of these disciplinary measures shall be appropriately documented.	HR-01.5H

A.6.1.3 Guidance requirements

- External references are needed, in particular ISO27005 for the terminology and ISO31000 for the methodology.

A.6.2 HR-02 Verification of Qualification and Trustworthiness

A.6.2.1 Objective

The competence 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.

A.6.2.2 Requirements

Basic	The <u>CSP</u> shall assess the <u>competence</u> and integrity of all its <u>personnel</u> with access to <u>CSC data</u> or <u>system components</u> under the <u>CSP's</u> responsibility, or who are responsible to provide the <u>cloud service</u> in the <u>production environment</u> before commencement of employment in a position classified in <u>objective</u> HR-01.	HR-02.1B
	The <u>CSP</u> shall assess the <u>competence</u> and integrity of its <u>personnel</u> before commencement of employment in a position with a higher <u>risk</u> classification that their previous position within the company.	HR-02.2B
	The extent of the assessment defined in HR-02.1B and HR-02.2B shall be proportional to the business context, the sensitivity of the information that will be accessed by the <u>personnel</u> , and the associated <u>risks</u> .	HR-02.3B
Substantial	The <u>CSP</u> shall assess the <u>competence</u> and integrity of all its <u>personnel</u> with access to <u>CSC data</u> or <u>system components</u> under the <u>CSP's</u> responsibility, or who are responsible to provide the <u>cloud service</u> in the <u>production environment</u> before commencement of employment in a position classified in <u>objective</u> HR-01.	HR-02.1S
	The <u>CSP</u> shall assess the <u>competence</u> and integrity of its <u>personnel</u> of the <u>CSP</u> before commencement of employment in a position with a higher <u>risk</u> classification that their previous position within the company.	HR-02.2S
	The extent of the assessment defined in HR-02.1S and HR-02.2S shall be proportional to the business context, the sensitivity of the information that will be accessed by the <u>personnel</u> , and the associated <u>risks</u> .	HR-02.3S
High	The <u>CSP</u> shall assess the <u>competence</u> and integrity of all its <u>personnel</u> with access to <u>CSC data</u> or <u>system components</u> under the <u>CSP's</u> responsibility, or who are responsible to provide the <u>cloud service</u> in the <u>production environment</u> before commencement of employment in a position classified in <u>objective</u> HR-01.	HR-02.1H

	The CSP shall assess the competence and integrity of its personnel of the CSP before commencement of employment in a position with a higher <u>risk</u> classification than their previous position within the company.	HR-02.2H
	The extent of the assessment defined in HR-02.1H and HR-02.2H shall be proportional to the business context, the sensitivity of the information that will be accessed by the <u>personnel</u> , and the associated <u>risks</u> .	HR-02.3H
	The CSP shall review annually their assessment of the competence and integrity of its personnel for the individuals in positions with the highest levels of <u>risk</u> classification, starting at a level to be defined in the human resource <u>policy</u>	HR-02.4H

A.6.2.3 Guidance requirements

- The risk-based approach in HR-02.1 should be based on a variety of parameters, including the data accessible by employees, the privileges assigned to employees, including in particular administration rights for the systems that provide the cloud service.
- The review performed in HR-02.1 should be tracked and archived, to be made available to an auditor.
- The agreement should at least stipulate that for any matter related to the security of the cloud service:
 - professional duties are performed with loyalty, discretion and impartiality; and
 - Internal and external employees use only those methods, tools and techniques that have been approved by the CSP.
- For higher levels, the following areas should also be included:
 - Request of a police clearance certificate for applicants; and
 - Evaluation of the risk to be blackmailed (from C5, be careful in wording).

A.6.3 HR-03 Employee Terms and Conditions

A.6.3.1 Objective

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

A.6.3.2 Requirements

Basic	The CSP shall ensure that all <u>personnel</u> are required by their terms and conditions to comply with all applicable <u>information security policies</u> and <u>procedures</u> .	HR-03.1B
	The CSP shall ensure that the terms for all <u>personnel</u> include a non-disclosure provision.	HR-03.2B
	The non-disclosure provision shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	HR-03.3B
	The CSP shall give a presentation of all applicable <u>information security policies</u> and <u>procedures</u> to <u>personnel</u> before granting them any access to <u>CSC data</u> , the <u>production environment</u> , or any <u>functional component</u> thereof.	HR-03.4B
Substantial	The CSP shall ensure that all <u>personnel</u> are required by their terms and conditions to comply with all applicable <u>information security policies</u> and <u>procedures</u> .	HR-03.1S
	The CSP shall ensure that the terms for all <u>personnel</u> include a non-disclosure provision.	HR-03.2S
	The non-disclosure provision shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	HR-03.3S
	The CSP shall give a presentation of all applicable <u>information security policies</u> and <u>procedures</u> to <u>personnel</u> before granting them any access to <u>CSC data</u> , the <u>production environment</u> , or any <u>functional component</u> thereof.	HR-03.4S
	All <u>personnel</u> shall acknowledge in a documented form the <u>information security policies</u> and <u>procedures</u> presented to them before they are granted any access to <u>CSC data</u> , the <u>production environment</u> , or any <u>functional component</u> thereof.	HR-03.5S
High	The CSP shall ensure that all <u>personnel</u> are required by their terms and conditions to comply with all applicable <u>information security policies</u> and <u>procedures</u> .	HR-03.1H

	The CSP shall ensure that the terms for all personnel include a non-disclosure provision.	HR-03.2H
	The non-disclosure provision shall cover any information that has been obtained or generated as part of the cloud service, even if anonymised and decontextualized.	HR-03.3H
	The CSP shall give a presentation of all applicable information security policies and procedures to personnel before granting them any access to CSC data, the production environment, or any functional component thereof.	HR-03.4H
	All personnel shall acknowledge in a documented form the information security policies and procedures presented to them before they are granted any access to CSC data, the production environment or any functional component thereof.	HR-03.5H
	The verification of this acknowledgement shall be automatically monitored in the processes used to grant access rights to personnel.	HR-03.6H

A.6.3.3 Guidance requirements

- Some guidance about how monitoring can be applied here.

A.6.4 HR-04 Security Awareness and Training

A.6.4.1 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.

A.6.4.2 Requirements

Basic	<p>The CSP shall define a security awareness and training program that covers the following aspects:</p> <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 CSC data in accordance with applicable policies and procedures and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents <p>The CSP shall review their security awareness and training program based on changes to policies and procedures and the current threat situation.</p> <p>The CSP shall ensure that all personnel complete the security awareness and training program defined for them.</p>	<p>HR-04.1B</p> <p>HR-04.2B</p> <p>HR-04.3B</p>
Substantial	<p>The CSP shall define a security awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties, and that covers the following aspects:</p> <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 CSC data in accordance with applicable policies and procedures and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents. <p>The CSP shall review their security awareness and training program at least annually, and based on changes to policies and instructions and the current threat situation.</p> <p>The CSP shall ensure that all personnel complete the security awareness and training program defined for them at least annually, and when changing target group.</p> <p>The CSP shall measure and evaluate the learning outcomes achieved through the awareness and training programme.</p>	<p>HR-04.1S</p> <p>HR-04.2S</p> <p>HR-04.3S</p> <p>HR-04.4S</p>
High	<p>The CSP shall define a security awareness and training program on a target group-oriented manner, taking into consideration at least the position's risk classification and technical duties, and that covers the following aspects:</p> <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; 	HR-04.1H

	<ul style="list-style-type: none"> Handling CSC data in accordance with applicable <u>policies</u> and <u>procedures</u> and applicable legal and regulatory <u>requirements</u>; Information about the current <u>threat</u> situation; and Correct behaviour in the event of <u>security incidents</u>. 	
	The CSP shall <u>review</u> their security awareness and training program at least annually, and based on changes to <u>policies</u> and <u>instructions</u> and the current <u>threat</u> situation.	HR-04.2H
	The CSP shall ensure that all <u>personnel</u> complete the security awareness and training program defined for them at least annually, and when changing target group.	HR-04.3H
	The CSP shall automatically <u>monitor</u> the completion of the security awareness and training program.	HR-04.5H
	The CSP shall measure and evaluate in a <u>target group-oriented manner</u> the learning outcomes achieved through the awareness and training programme.	HR-04.4H
	The measurements shall cover quantitative and qualitative aspects.	HR-04.6H
	The results of the measurements shall be used to improve the awareness and training programme.	HR-04.7H

A.6.4.3 Guidance requirements

-

A.6.5 HR-05 Termination or Change in Employment

A.6.5.1 Objective

Internal and external employees have been informed about which responsibilities, arising from the policies and procedures 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.

A.6.5.2 Requirements

Basic	The CSP shall communicate to personnel their ongoing responsibilities relating to <u>information security</u> when their employment is terminated or changed.	HR-05.1B
	The CSP shall apply a specific <u>procedure</u> to revoke the <u>access rights</u> and process appropriately the accounts and <u>assets</u> of <u>personnel</u> when their employment is terminated or changed.	HR-05.2B
Substantial	The CSP shall communicate to personnel their ongoing responsibilities relating to <u>information security</u> when their employment is terminated or changed.	HR-05.1S
	The CSP shall apply a specific <u>procedure</u> to revoke the <u>access rights</u> and process appropriately the accounts and <u>assets</u> of <u>personnel</u> when their employment is terminated or changed, defining specific roles and responsibilities and including a documented checklist of all required steps.	HR-05.2S
High	The CSP shall communicate to personnel their ongoing responsibilities relating to <u>information security</u> when their employment is terminated or changed.	HR-05.1H
	The CSP shall apply a specific <u>procedure</u> to revoke the <u>access rights</u> and process appropriately the accounts and <u>assets</u> of <u>personnel</u> when their employment is terminated or changed, defining specific <u>roles</u> and responsibilities and including a documented checklist of all required steps.	HR-05.2H
	The CSP shall automatically <u>monitor</u> the application of this <u>procedure</u>.	HR-05.3H

A.6.5.3 Guidance requirements

- The revocation is expected to have immediate effect (before the actual employee's departure)

A.6.6 HR-06 Confidentiality Agreements

A.6.6.1 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.

A.6.6.2 Requirements

Basic	The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with <u>employees</u> <u>external service providers</u> and <u>suppliers</u> .	HR-06.1B
Substantial	The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with <u>employees</u> , <u>external service providers</u> and <u>suppliers</u> , based on the requirements identified by the CSP for the protection of confidential information and operational details .	HR-06.1S
	Acceptance of the agreements by external service providers and suppliers shall take place when the contract is agreed.	HR-06.2S
	Acceptance of the agreements by employees of the CSP shall take place before authorisation to access CSC data is granted.	HR-06.3S
	The requirements on which the agreements are based shall be documented and reviewed at regular intervals, at least annually.	HR-06.4S
	The CSP shall inform its employees and obtain confirmation of their acceptance of the updated confidentiality or non-disclosure agreement.	HR-06.5S
High	The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with <u>employees</u> , <u>external service providers</u> and <u>suppliers</u> , based on the <u>requirements</u> identified by the CSP for the protection of confidential information and operational details.	HR-06.1H
	The agreements shall be accepted by external <u>service providers</u> and <u>suppliers</u> when the contract is agreed.	HR-06.2H
	The acceptance of agreements by external service providers and suppliers shall be automatically monitored.	HR-06.6H
	The agreements shall be accepted by <u>employees</u> of the CSP before authorisation to access CSC data is granted.	HR-06.3H
	The acceptance of agreements by shall be automatically monitored.	HR-06.7H
	The <u>requirements</u> on which the agreements are based shall be <u>documented</u> and <u>reviewed</u> at regular intervals, at least annually; if the review shows that the requirements need to be modified, then the non-disclosure or confidentiality agreements shall be modified accordingly.	HR-06.4H
	The CSP shall inform its <u>employees</u> and obtain confirmation of their acceptance of the updated confidentiality or non-disclosure agreement.	HR-06.5H
	The acceptance of updated agreements shall be automatically monitored.	HR-06.8H

A.6.6.3 Guidance requirements

-

A.7 ASSET MANAGEMENT

IDENTIFY THE ORGANISATION'S OWN ASSETS AND ENSURE AN APPROPRIATE LEVEL OF PROTECTION THROUGHOUT THEIR LIFE CYCLE.

Term	Definition
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, 3.2.1]</p>
asset life	<p>period from asset creation to asset end-of-life</p> <p>[SOURCE: From ISO55000, 3.2.2]</p>
asset 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, 3.2.3]</p>
asset system	<p>set of assets that interact or are interrelated</p> <p>[SOURCE: From ISO55000, 3.2.5]</p>

A.7.1 AM-01 Asset Inventory

A.7.1.1 Objective

The CSP has established procedures for inventorying assets, including all IT to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle.

A.7.1.2 Requirements

Basic	The CSP shall define and implement policies and procedures for maintaining an inventory of assets that are used to provide the cloud service.	AM-01.1B
	The CSP shall add in the record for each asset the information needed to apply the risk management procedure defined in RM-01.	AM-01.2B
Substantial	The CSP shall define and implement policies and procedures for maintaining an inventory of assets that are used to provide the cloud service.	AM-01.1S
	The inventory shall be performed automatically or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset life cycle.	AM-01.3S
	The CSP shall add in the record for each asset the information needed to apply the risk management procedure defined in RM-01.	AM-01.2S
	The CSP shall review the risk treatment plan according to RM-03 throughout the life cycle of the asset included in the risk assessment.	AM-01.4S

High	The CSP shall <u>define</u> and implement policies and <u>procedures</u> for maintaining an inventory of <u>assets</u> that are used to provide the <u>cloud service</u> .	AM-01.1H
	The inventory shall be performed automatically or by the people or teams responsible for the <u>assets</u> to ensure complete, accurate, valid and consistent inventory throughout the <u>asset life cycle</u> .	AM-01.3H
	The CSP shall add in the record for each <u>asset</u> the information needed to apply the <u>risk management procedure</u> defined in RM-01.	AM-01.2H
	The CSP shall <u>review</u> the <u>risk treatment plan</u> according to RM-03 throughout the <u>life cycle</u> of the <u>asset</u> included in the <u>risk assessment</u> .	AM-01.4H
	The <u>information about assets</u> shall be considered for their <u>impact on cloud services</u> in case of a breach of <u>information security requirements</u> that affect <u>cloud customers</u> in accordance with contractual agreements.	AM-01.5H
	The CSP shall automatically monitor the process that is maintaining the inventory of <u>assets</u> to guarantee it is up-to-date in accordance with contractual agreements.	AM-01.6H

A.7.1.3 Guidance requirements

- 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.
- Automation should be the favourite way (over manual inventory), also for efficiency/cost reasons
- The information recorded should include:
 - the information for identifying the asset
 - the function of the asset;
 - the model and version of the asset;
 - the location of the asset;
- The CSP should log at least all changes to the information related to risk management on each asset

A.7.2 AM-02 Acceptable Use and Safe Handling of Assets Policy

A.7.2.1 Objective

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

A.7.2.2 Requirements

Basic	The CSP shall <u>define</u> and implement policies and <u>procedures</u> as defined in ISP-02 for acceptable use and safe handling of <u>assets</u> .	AM-02.1B
	The use of removable media shall be forbidden except for unavoidable essential system administration tasks, and then only in the event that no other mechanism is possible.	AM-02.2B
	When removable media is used in the situations described in AM-02.1, this media shall be dedicated to a single purpose.	AM-02.3B
	The decision to use removable media shall be documented.	AM-02.4B
Substantial	The CSP shall <u>define</u> and implement policies and <u>procedures</u> as defined in ISP-02 for acceptable use and safe handling of <u>assets</u> .	AM-02.1S
	The use of removable media shall be forbidden except for unavoidable essential system administration tasks, and then only in the event that no other mechanism is possible.	AM-02.2S
	When removable media is used in the situations described in AM-02.1, this media shall be dedicated to a single purpose.	AM-02.3S
	The decision to use removable media shall be documented.	AM-02.4S
High	The CSP shall <u>define</u> and implement policies and <u>procedures</u> as defined in ISP-02 for acceptable use and safe handling of <u>assets</u> .	AM-02.1H

	The use of removable media shall be forbidden except for unavoidable essential system administration tasks, and then only in the event that no other mechanism is possible.	AM-02.2H
	When removable media is used in the situations described in AM-02.1, this media shall be dedicated to a single purpose.	AM-02.3H
	The decision to use removable media shall be documented.	AM-02.4H

A.7.2.3 Guidance requirements

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

A.7.3 AM-03 Commissioning and Decommissioning

A.7.3.1 Objective

Procedures for the commissioning and decommissioning of hardware assets used in the provision of the cloud service are documented, communicated and implemented, ensuring the proper configuration before commissioning and the proper deletion of data during decommissioning..

A.7.3.2 Requirements

Basic	The CSP shall define 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.	AM-03.1B
	The CSP shall define and implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment including the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies.	AM-03.2B
Substantial	The CSP shall define 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 including those defined in RM-01, to ensure that the risks arising from the commissioning are identified, analysed and mitigated.	AM-03.1S
	The commissioning procedure shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and	AM-03.3S

	<p>authorisation according to the intended use and based on the applicable policies, before authorisation to commission the asset can be granted.</p> <p>The CSP shall define and implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, including the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies.</p>	AM-03.2S
High	<p>The CSP shall define 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, including those defined in RM-01, to ensure that the risks arising from the commissioning are identified, analysed and mitigated.</p> <p>The commissioning procedure shall include verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies, before authorisation to commission the asset can be granted.</p> <p>The CSP shall define and implement a procedure for the decommissioning of hardware that is used to provide the cloud service in the production environment, including the complete and permanent deletion of the data or the proper destruction of the media and requiring approval based on applicable policies.</p> <p>The approval of the commissioning and decommissioning of hardware shall be digitally documented and automatically monitored.</p>	<p>AM-03.1H</p> <p>AM-03.3H</p> <p>AM-03.2H</p> <p>AM-03.4H</p>

A.7.3.3 Guidance requirements

- Explain applicability to assets (hardware, plus virtual assets for OPS and DEV)

A.7.4 AM-04 Acceptable Use, Safe Handling and Return of Assets

A.7.4.1 Objective

The CSP's internal and external employees are provably committed to the policies and procedures for acceptable use and safe handling of assets before they can be used if the CSP 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.

A.7.4.2 Requirements

Basic	<p>The CSP shall ensure and document that all personnel are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02.</p> <p>The procedure mentioned in HR-06.2 shall include steps to ensure that all assets under custody of an personnel are returned upon termination of employment.</p>	<p>AM-04.1B</p> <p>AM-04.2B</p>
Substantial	<p>The CSP shall ensure and document that all personnel are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02.</p> <p>The procedure mentioned in HR-06.2 shall include steps to ensure that all assets under custody of an personnel are returned upon termination of employment.</p>	<p>AM-04.1S</p> <p>AM-04.2S</p>
High	<p>The CSP shall ensure and document that all personnel are committed to the policies and procedures for acceptable use and safe handling of assets in the situations described in AM-02.</p> <p>This commitment shall be automatically monitored.</p> <p>The procedure mentioned in HR-06.2 shall include steps to ensure that all assets under custody of an personnel are returned upon termination of employment.</p> <p>The CSP shall centrally manage the assets under the custody of personnel, including asset distribution, data and software licences, appropriately using remote deactivation, deletion or locking, of related hardware or software.</p>	<p>AM-04.1H</p> <p>AM-04.4H</p> <p>AM-04.2H</p> <p>AM-04.3H</p>

A.7.4.3 Guidance requirements

- Central management of assets should be considered at all levels

A.7.5 AM-05 Asset Classification and Labelling

A.7.5.1 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.

A.7.5.2 Requirements

Basic	<p>The CSP shall document an asset classification schema that reflects for each asset the protection needs of the information it embodies or may process, store, or transmit.</p> <p>When applicable, the CSP shall label all assets according to their classification in the asset classification schema.</p>	<p>AM-05.1B</p> <p>AM-05.2B</p>
Substantial	<p>The CSP shall document an asset classification schema that reflects for each asset the protection needs of the information it embodies or may process, store, or transmit, and provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.</p> <p>When applicable, the CSP shall label all assets according to their classification in the asset classification schema.</p> <p>The need for protection shall be determined by the individuals or groups responsible for the assets</p>	<p>AM-05.1S</p> <p>AM-05.2S</p> <p>AM-05.3S</p>
High	<p>The CSP shall document an asset classification schema that reflects for each asset the protection needs of the information it embodies or may process, store, or transmit, and provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.</p> <p>When applicable, the CSP shall label all assets according to their classification in the asset classification schema.</p> <p>The need for protection shall be determined by the individuals or groups responsible for the assets.</p>	<p>AM-05.1H</p> <p>AM-05.2H</p> <p>AM-05.3H</p>

A.7.5.3 Guidance requirements

- Definition of a label: "The means used to associate a set of security attributes with an asset". Note that labelling is not necessarily physical.
- Also introduce the notion of need for protection

A.8 PHYSICAL SECURITY

PREVENT UNAUTHORISED PHYSICAL ACCESS AND PROTECT AGAINST THEFT, DAMAGE, LOSS AND OUTAGE OF OPERATIONS.

Term	Definition
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

A.8.1 PS-01 Physical Security Perimeters

A.8.1.1 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.

A.8.1.2 Requirements

Basic	The CSP shall define <u>security perimeters</u> in the buildings and premises related to the <u>cloud service</u> provided.	PS-01.1B
	The CSP shall define at least two <u>security areas</u> with at least one sensitive area covering sensitive <u>activities</u> such as the buildings and premises hosting the information system for the provision of the <u>cloud service</u> , and at least one public area covering at least all remaining buildings and premises.	PS-01.2B
	The CSP shall define and implement a set of security <u>requirements</u> for each <u>security area</u> in a <u>policy</u> and <u>procedures</u> according to ISP-02.	PS-01.3B
Substantial	The CSP shall define <u>security perimeters</u> in the buildings and premises related to the <u>cloud service</u> provided.	PS-01.1S
	The CSP shall define at least two <u>security areas</u> , with at least one sensitive area covering sensitive <u>activities</u> such as the buildings and premises hosting the information system for the provision of the <u>cloud service</u> , and at least one public area covering at least all remaining buildings and premises.	PS-01.2S
	The CSP shall define and implement a set of security <u>requirements</u> for each <u>security area</u> in a <u>policy</u> and <u>procedures</u> according to ISP-02, <u>based on the security objectives of the information security policy</u> , <u>identified protection requirements for the cloud service</u> and the <u>assessment of risks</u> to physical and environmental security.	PS-01.3S
High	The CSP shall define <u>security perimeters</u> in the buildings and premises related to the <u>cloud service</u> provided.	PS-01.1H
	The CSP shall define at least three <u>security areas</u> , with at least one sensitive area covering sensitive <u>activities</u> such as the buildings and premises hosting the information system for the provision of the <u>cloud service</u> , at least one additional private area that may host development activities and administration, supervision and operation workstations. and at least one public area covering at least all remaining buildings and premises.	PS-01.2H
	The CSP shall ensure that no direct access exists between a public area and a sensitive area, without going through a private area.	PS-01.4H

	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.	PS-01.5H
	The CSP shall define and implement a set of security requirements for each security area in a policy and procedures according to ISP-02, 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.	PS-01.3H

A.8.1.3 Guidance requirements

- Refine the definition of the different perimeters in guidance.
- Include guidance how perimeters and areas can be defined, in particular for SMEs, with a link to the access control requirements.
- Also include guidance about the potential use of “work from home” settings in the various zones (typically, allowed for public, strictly controlled for private, and none for sensitive)

A.8.2 PS-02 Physical Site Access Control

A.8.2.1 Objective

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

A.8.2.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 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.	PS-02.1B
	The access control policy shall require at least one authentication factor for accessing any non-public area.	PS-02.2B
	The access control policy shall describe the physical access control derogations in case of emergency, including an analysis procedure after every use of these derogations.	PS-02.3B
	The CSP shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to the corresponding areas.	PS-02.4B
	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.	PS-02.5B
Substantial	The CSP shall define and implement policies and procedures according to ISP-02 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, including requirements on the physical access control measures to be implemented.	PS-02.1S
	The access control policy shall require at least one authentication factor for accessing any non-public area, and at least two distinct kinds of authentication factors for accessing any sensitive area and areas hosting system components that process CSC data.	PS-02.2S
	The access control policy shall describe the physical access control derogations in case of emergency, including an analysis procedure after every use of these derogations.	PS-02.3S
	The CSP shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to the corresponding areas.	PS-02.4S
	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.	PS-02.5S
	The access control policy shall include requirements concerning preventive and detective physical access control.	PS-02.6S
	The access control policy shall include measures to identify individuals who are not part of the personnel incorporating them into the access policy system, thereby monitoring and escorting the building access during their stay.	PS-02.7S
	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 areas.	PS-02.8S

High	The CSP shall <u>define and implement policies and procedures</u> according to ISP-02 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, including <u>requirements on the physical access control measures</u> to be implemented.	PS-02.1H
	The access control policy shall require at least one authentication factor for accessing any non-public area, and at least two authentication factors for accessing any sensitive area and areas hosting system components that process CSC data.	PS-02.2H
	The physical access control policy shall describe the time slots and conditions for accessing each security area according to the profiles of the users.	PS-02.9H
	The access control policy shall describe the physical <u>access control</u> derogations in case of emergency.	PS-02.3H
	The CSP shall display at the entrance of all non-public perimeters a warning concerning the limits and access conditions to the corresponding areas.	PS-02.4H
	The CSP shall protect security perimeters with security measures to detect and prevent unauthorised access in a demonstrated timely manner so that it does not compromise the information security of the cloud service.	PS-02.5H
	The access control policy shall include <u>requirements</u> concerning preventive and detective physical access control.	PS-02.6H
	The access control policy shall include measures to identify individuals who are not part of the personnel, incorporating them into the <u>access policy</u> system, thereby monitoring and escorting the building access during their stay.	PS-02.7H
	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 areas.	PS-02.8H
	This logging shall be automatically monitored .	PS-02.10H

A.8.2.3 Guidance requirements

- A mix of prevention and detection measures are possible, and “timely” must be defined in greater details for each level.
- List possible ways to perform a “loggable” access control.

A.8.3 PS-03 Working in Non-public Areas

A.8.3.1 Objectives

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

A.8.3.2 Requirements

Basic	The CSP shall <u>define and implement policies and procedures</u> according to ISP-02 concerning work in non-public areas.	PS-03.1B
Substantial	The CSP shall define and implement policies and procedures according to ISP-02 concerning work in non-public areas, including at least a <u>clear screen policy</u> and a <u>clear desk policy</u> for sensitive information and removable media.	PS-03.1S
	If visitors need to access a non-public area, the CSP shall ensure that they are supervised by <u>personnel</u> who have been authorised (cf. HR-02.1S), who will follow the visitors, authorise or deny their actions, and question them if needed about their actions.	PS-03.2S

High	The CSP shall define and implement policies and procedures according to ISP-02 concerning work in non-public areas, including at least a clear screen policy and a clear desk policy for sensitive information and removable media.	PS-03.1H
	The CSP shall define a mapping between activities and security areas that indicates which activities may/shall not/shall be performed in every security area.	PS-03.3H
	The CSP shall define a mapping between assets and security areas that indicates which assets may/shall not/shall be used in every security area.	PS-03.4H
	If visitors need to access a non-public area, the CSP shall ensure that they are supervised by personnel who have been authorised (cf. HR-02.1H), who will follow the visitors, authorise or deny their actions, and question them if needed about their actions.	PS-03.2H

A.8.3.3 Guidance requirements

- The clear screen policy may define exceptions for specific areas with restricted access, or specific policies for “work from home”.

A.8.4 PS-04 Equipment Protection

A.8.4.1 Objectives

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

A.8.4.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 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 CSC data during transport. 	PS-04.1B
	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.	PS-04.2B
Substantial	The CSP shall define and implement policies and procedures according to ISP-02 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 CSC data during transport. 	PS-04.1S
	These procedures shall include at least: <ul style="list-style-type: none"> 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; a procedure for transferring any equipment containing CSC 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. 	PS-04.3S
	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.	PS-04.2S
	The CSP shall ensure that an equipment containing a media with CSC data can be returned to a third party only if the CSC data stored on it is encrypted in accordance with CKM-03 or has been destroyed beforehand using a secure deletion mechanism.	PS-04.4S

High	The CSP shall <u>define</u> and <u>implement</u> policies and <u>procedures</u> according to ISP-02 concerning the protection of equipment and including at least the following aspects:	PS-04.1H
	<ul style="list-style-type: none"> Protecting power and communications cabling from interception, interference or damage; Protecting equipment during maintenance operations; Protecting equipment holding CSC data during transport. 	
	These <u>procedures</u> shall include at least:	PS-04.3H
	<ul style="list-style-type: none"> a <u>procedure</u> 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; a procedure for transferring any equipment containing CSC 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, including a formal validation by top management of the CSP or by the authorized body that validated this procedure; a <u>procedure</u> to <u>maintain</u> and keep up-to-date a wiring scheme; 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 <u>cloud service's</u> availability and security <u>requirements</u>. 	(a) (b) (c) (d)
	The CSP shall use encryption on all removable media and backup media intended to move between security areas.	PS-04.2H
	The CSP shall ensure that an equipment containing a media with CSC data can be returned to a <u>third party</u> only if the CSC data stored on it is encrypted in accordance with CKM-03 or has been destroyed beforehand using a secure deletion mechanism.	PS-04.4H
	The CSP shall ensure that the maintenance agreements for equipment used to host the <u>cloud service</u> make it possible to have security updates installed in timely fashion on this equipment.	PS-04.5H

A.8.4.3 Guidance requirements

- The checks to be performed for the protection of cables should include at least the following aspects:
 - Traces of violent attempts to open closed distributors;
 - Up-to-datedness of the documentation in the distribution list;
 - Conformity of the actual wiring and patching with the documentation;
 - The short-circuits and earthing of unneeded cables are intact; and
 - Impermissible installations and modifications.
- Provide an explanation of the perimeter of cabling that needs to be checked, focusing on the cabling that is included in the premises, and explaining that cables outside of that scope should be considered as publicly accessible, leading to constraints on data in motion.

A.8.5 PS-05 Protection against External and Environmental Threats

A.8.5.1 Objective

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

A.8.5.2 Requirements

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

A.8.5.3 Traceability / Rationale

Source	Traceability / Rationale
C5:2020 PS-01	<ul style="list-style-type: none"> C5:PS-01 introduces the requirement for a policy on environmental control (PS-05.1B) and for the use of established technologies in data centres (PS-05.2S) C5:PS-01 defines additional criteria for data centres (PS-05.2H)
C5:2020 PS-02	<ul style="list-style-type: none"> C5:PS-02 introduces the requirement for operating in 2 locations (PS-05.3S) and for testing the redundancy (PS-05.4S)
SecNumCloud:3.0 11	<ul style="list-style-type: none"> SecNumCloud:11.3 introduces a testing requirement for data centres (PS-05.2H).

A.8.5.4 Guidance requirements

- The “established rules of technology” for datacentres will be refined in guidance
- 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.
- Force majeure may have an impact on physical access control, for instance as staff may not be able to reach the premises and alternate workers need to be authorized.

A.9 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

Term	Definition
capacity management	process for monitoring, analysis, reporting and improvement of capacity [SOURCE: From ISO/IEC TS 22237-7:2018, 3.1.2]
malware malicious software	malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability Note 1 to entry: Viruses and Trojan horses are examples of malware. [SOURCE: ISO/IEC 27033-1:2015, 3.22]
events log	log which records audit trail data related to the system operations [SOURCE: From ISO 14641:2018, 3.2]
vulnerability	weakness of an asset or control that can be exploited by one or more threats [SOURCE: From ISO27000:2018, 3.77]
derived data 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. [SOURCE: From ISO17788:2014, 3.2.13]
penetration testing	Authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. [SOURCE: Adapted from Wikipedia]

A.9.1 OPS-01 Capacity Management – Planning

A.9.1.1 Objective

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

A.9.1.2 Requirements

Basic	The CSP shall <u>define and implement procedures</u> to plan for capacities and resources (personnel and IT resources).	OPS-01.1B
	The procedures shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.	OPS-01.2B
	The CSP shall meet the <u>requirements</u> included in contractual agreements with <u>CSCs</u> regarding the provision of the cloud service in case of capacity bottlenecks or personnel and IT resources outages.	OPS-01.3B

Substantial	The CSP shall <u>define and implement procedures</u> to plan for capacities and resources (personnel and IT resources).	OPS-01.1S
	The procedures shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.	OPS-01.2S
	The CSP shall meet the <u>requirements</u> included in contractual agreements with <u>CSCs</u> regarding the provision of the <u>cloud service</u> in case of capacity bottlenecks or personnel and IT resources outages.	OPS-01.3S
High	The CSP shall <u>define and implement procedures</u> to plan for capacities and resources (personnel and IT resources).	OPS-01.1H
	The procedures shall include forecasting future capacity requirements in order to identify usage trends and manage system overload.	OPS-01.2H
	Projected capacity requirements used for planning and provisioning preparation shall allow for the service level agreements.	OPS-01.4H
	The CSP shall meet the <u>requirements</u> included in contractual agreements with <u>CSCs</u> regarding the provision of the <u>cloud service</u> in case of capacity bottlenecks or personnel and IT resources outages.	OPS-01.3H

A.9.1.3 Guidance requirements

- Provide further information about the procedures to plan capacities.
- Mention that the CSP, through its contracts, ensures that it has access to additional capacity building components (e.g. hardware, networking components) in case of unexpected customer demand – 'High'

A.9.2 OPS-02 Capacity Management – Monitoring

A.9.2.1 Objective

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

A.9.2.2 Requirements

Basic	The CSP shall document and implement technical and organizational safeguards for the <u>monitoring</u> of provisioning and de-provisioning of <u>cloud services</u> to ensure compliance with the service level agreement.	OPS-02.1B
Substantial	The CSP shall document and implement technical and organizational safeguards for the <u>monitoring</u> of provisioning and de-provisioning of <u>cloud services</u> to ensure compliance with the service level agreement.	OPS-02.1S
High	The CSP shall document and implement technical and organizational safeguards for the <u>monitoring</u> of provisioning and de-provisioning of <u>cloud services</u> to ensure compliance with the service level agreement.	OPS-02.1H
	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of these safeguards.	OPS-02.2H
	The CSP shall make available to the <u>CSC</u> the relevant information regarding capacity and availability.	OPS-02.3H

A.9.2.3 Guidance requirements

- Provide further information on the information to be made available to customers.

A.9.3 OPS-03 Capacity Management – Controlling of Resources

A.9.3.1 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.

A.9.3.2 Requirements

Basic	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.	OPS-03.1B
Substantial	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.	OPS-03.1S
High	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.	OPS-03.1H

A.9.3.3 Guidance requirements

-

A.9.4 OPS-04 Protection against Malware – Policies

A.9.4.1 Objective

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

A.9.4.2 Requirements

Basic	<p>The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects:</p> <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 personnel's terminal equipment 	OPS-04.1B
Substantial	<p>The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects:</p> <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 personnel's terminal equipment <p>The CSP shall create regular reports on the malware checks performed.</p> <p>These reports on malware checks shall be assessed and analysed in the reviews of the policies related to malware.</p> <p>The CSP shall update the anti-malware products according to established policies and procedures ensuring a timely update.</p>	<p>OPS-04.1S</p> <p>OPS-04.2S</p> <p>OPS-04.3S</p> <p>OPS-04.4S</p>
High	<p>The CSP shall define and implement policies and procedures according to ISP-02 to protect its systems and its customers from malware, covering at least the following aspects:</p> <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; 	OPS-04.1H

	<ul style="list-style-type: none"> Operation of protection programs for <u>personnel's</u> terminal equipment <p>The CSP shall create regular reports on the malware checks performed.</p> <p>These reports on malware checks shall be assessed and analysed in the <u>reviews</u> of the policies related to malware.</p> <p>The CSP shall <u>update</u> the anti-malware products according to established <u>policies</u> and <u>procedures</u> ensuring a timely update at the highest appropriate frequency consistent with the risk assessment.</p>	OPS-04.2H OPS-04.3H OPS-04.4H
--	---	-------------------------------------

A.9.4.3 Guidance requirements

- Define the "authorized bodies" who review the reports on malware checks

A.9.5 OPS-05 Protection against Malware – Implementation

A.9.5.1 Objective

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

A.9.5.2 Requirements

Basic	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the <u>production environment</u> , according to <u>policies</u> and <u>procedures</u> .	OPS-05.1B
Substantial	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the <u>production environment</u> , according to <u>policies</u> and <u>procedures</u> .	OPS-05.1S
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available.	OPS-05.2S
High	The CSP shall deploy malware protection, if technically feasible, on all systems that support delivery of the cloud service in the <u>production environment</u> , according to <u>policies</u> and <u>procedures</u> .	OPS-05.1H
	Signature-based and behaviour-based malware protection tools shall be updated at least daily, if an update is available.	OPS-05.2H
	The CSP shall automatically monitor the systems covered by the malware protection and the configuration of the corresponding mechanisms to guarantee fulfilment of above requirements, and the antimalware scans to track detected malware or irregularities.	OPS-05.3H

A.9.5.3 Guidance requirements

- Define various malware protection methods, that may go beyond "antivirus" and include alternative methods of detecting unwarranted changes in the software or firmware of systems

A.9.6 OPS-06 Data Backup and Recovery – Policies

A.9.6.1 Objective

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

A.9.6.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 for data backup and recovery.	OPS-06.1B
Substantial	<p>The CSP shall define and implement policies and procedures according to ISP-02 for data backup and recovery, covering at least the following aspects:</p> <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 CSCs and the CSP's operational continuity requirements for recovery time objective (RTO) and recovery point objective (RPO); • How data is backed up in encrypted, state-of-the-art form; • How backup data is stored, moved, managed, and disposed of; • How a CSC-initiated recovery or recovery test is performed; • Restricted access to the backed-up data and the execution of restores only by authorised persons; and • Tests of recovery procedures (cf. OPS-08). 	OPS-06.1S
High	<p>The CSP shall define and implement policies and procedures according to ISP-02 for data backup and recovery, covering at least the following aspects:</p> <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 CSCs and the CSP's operational continuity requirements for recovery time objective (RTO) and recovery point objective (RPO); • How data is backed up in encrypted, state-of-the-art form; • How backup data is stored, moved, managed, and disposed of; • How a CSC-initiated recovery or recovery test is performed; • Restricted access to the backed-up data and the execution of restores only by authorised persons; and • Tests of recovery procedures (cf. OPS-08). 	OPS-06.1H

A.9.6.3 Guidance requirements

-

A.9.7 OPS-07 Data Backup and Recovery – Monitoring

A.9.7.1 Objective

The proper execution of data backups is monitored.

A.9.7.2 Requirements

Basic	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.	OPS-07.1B
Substantial	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.	OPS-07.1S
High	<p>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.</p> <p>In order to check the proper application of these measures, the CSP shall automatically monitor their data backups.</p> <p>The CSP shall make information available to the CSCs for monitoring the execution of backups when the CSC uses backup services with the CSP.</p>	<p>OPS-07.1H</p> <p>OPS-07.2H</p> <p>OPS-07.3H</p>

A.9.7.3 Guidance requirements

- Provide additional information on key indicators to be monitored (backup done, timing, hot or cold, (...))

A.9.8 OPS-08 Data Backup and Recovery – Regular Testing

A.9.8.1 Objective

The proper restoration of data backups is regularly tested.

A.9.8.2 Requirements

Basic	<p>The CSP shall test the restore procedures at least annually.</p> <p>The CSP shall not use CSC data to perform the restore tests, but only data in test accounts controlled by CSP personnel for testing purposes.</p>	<p>OPS-08.1B</p> <p>OPS-08.2B</p>
Substantial	<p>The CSP shall test the restore procedures at least annually, including tests assessing if the specifications for the RTO and RPO agreed with the CSCs are met.</p> <p>The CSP shall not use CSC data to perform the restore tests, but only data in test accounts controlled by CSP personnel for testing purposes.</p> <p>The CSP shall thoroughly document restore tests, including the safe disposal of restored data.</p> <p>Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation.</p>	<p>OPS-08.1S</p> <p>OPS-08.2S</p> <p>OPS-08.3S</p> <p>OPS-08.4S</p>
High	<p>The CSP shall test the restore procedures at least annually, embedded in the CSP's business continuity management, including tests assessing if the specifications for the RTO and RPO agreed with the CSCs are met.</p> <p>The CSP shall not use CSC data to perform the restore tests, but only data in test accounts controlled by CSP personnel for testing purposes.</p> <p>The CSP shall thoroughly document restore tests, including the safe disposal of restored data.</p> <p>Any deviation from the specification during the restore test shall be reported to the CSP's responsible person for assessment and remediation.</p> <p>The CSP shall inform CSCs, at their request, of the results of the recovery tests.</p>	<p>OPS-08.1H</p> <p>OPS-08.2H</p> <p>OPS-08.3H</p> <p>OPS-08.4H</p> <p>OPS-08.5H</p>

A.9.8.3 Guidance requirements

- Provide guidance about the relationship to BCM for High
- Remind that testing is not allowed using customer data

A.9.9 OPS-09 Data Backup and Recovery – Storage

A.9.9.1 Objective

Backup data is stored at an appropriate remote location.

A.9.9.2 Requirements

Basic	<p>The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location.</p> <p>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).</p>	<p>OPS-03.1B</p> <p>OPS-03.2B</p>
-------	--	-----------------------------------

Substantial	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location, selected upon criteria of distance, recovery times and impact of disasters on backup and main sites.	OPS-03.1S
	The data classification of the original data shall be applied automatically to backups.	OPS-03.3S
	The security measures at the remote site shall have at least the same level as at the main site.	OPS-03.4S
	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).	OPS-03.2S
High	The CSP shall transfer backup data to a remote location or transport them on backup media to a remote location, selected upon criteria of distance, recovery times and impact of disasters on backup and main sites.	OPS-03.1H
	The data classification of the original data is applied automatically to backups.	OPS-03.3H
	The security measures at the remote site shall have at least the same level as at the main site.	OPS-03.4H
	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).	OPS-03.2H
	The transmission of the data shall be automatically monitored by the CSP to verify the execution of the backup.	OPS-03.5H

A.9.9.3 Guidance requirements

- Remind that a SaaS provider's office is remote from its IaaS provider's data centre, so that could work at least for Basic.
- The "level" requirements on backup storage facilities relate to the requirements associated to a given assurance level. A backup facility for a High cloud service should satisfy all requirements for High.

A.9.10 OPS-10 Logging and Monitoring – Policies

A.9.10.1 Objective

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

A.9.10.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility.	OPS-03.1B
Substantial	<p>The CSP shall define and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility, covering at least the following aspects:</p> <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; Definition of roles and responsibilities for setting up and monitoring logging; Definition of log data that may be transferred to CSCs and technical requirements of such log forwarding; Information about timestamps in event creation; Time synchronisation of system components; and Compliance with legal and regulatory frameworks. 	OPS-03.1S
High	<p>The CSP shall define and implement policies and procedures according to ISP-02 that govern the logging and monitoring of events on system components under its responsibility, covering at least the following aspects:</p> <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; Definition of roles and responsibilities for setting up and monitoring logging; 	OPS-03.1S

- Definition of log data that may be transferred to CSCs and technical requirements of such log forwarding;
- Information about timestamps in event creation;
- Time synchronisation of system components; and
- Compliance with legal and regulatory frameworks.

A.9.10.3 Guidance requirements

•

A.9.11 OPS-11 Logging and Monitoring – Derived Data Management

A.9.11.1 Objective

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

A.9.11.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 that govern the secure handling of cloud service derived data.	OPS-11.1B
Substantial	<p>The CSP shall define and implement policies and procedures according to ISP-02 that govern the secure handling of cloud service derived data, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Purpose for the collection and use of cloud service derived data beyond the operation of the cloud service, including purposes related to the implementation of security controls; • In the contexts that go beyond a single CSC, anonymisation of the data, or failing that deidentification of the data, to be used wherever feasible; • 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 cloud service derived data to CSCs according to contractual agreements. <p>The CSP shall list in the contractual agreement with the CSC all purposes for the collection of use of cloud service derived data that are not related to the universal requirements that apply inherently to all cloud services</p> <p>The universal requirements include satisfaction of law enforcement requests and implementation of: security controls; system monitoring tuning and service performance management; provision of support services; basic administration of customer relationships; and billing.</p>	<p>OPS-11.1S</p> <p>OPS-11.2S</p> <p>OPS-11.3S</p>
High	<p>The CSP shall define and implement policies and procedures according to ISP-02 that govern the secure handling of cloud service derived data, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Purpose for the collection and use of cloud service 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 cloud service derived data to CSCs according to contractual agreements. <p>The CSP shall list in the contractual agreement with the CSC all purposes for the collection of use of cloud service derived data that are not related to the universal requirements that apply inherently to all cloud services.</p> <p>The universal requirements include satisfaction of law enforcement requests and implementation of: security controls; system monitoring tuning and service performance management; provision of support services; basic administration of customer relationships; and billing..</p> <p>Cloud service derived data including log data, shall be taken into consideration in regulatory compliance assessments.</p>	<p>OPS-11.1H</p> <p>OPS-11.2H</p> <p>OPS-11.3H</p> <p>OPS-11.4H</p>

A.9.11.3 Guidance requirements

- Explain why this is introduced here (log data being such derived data)
- Mention GDPR in the regulatory compliance assessments

A.9.12 OPS-12 Logging and Monitoring – Identification of Events

A.9.12.1 Objective

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

A.9.12.2 Requirements

Basic	The CSP shall monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements.	OPS-12.1B
	The identified events shall be reported to the appropriate departments for timely assessment and remediation.	OPS-12.2B
Substantial	The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements.	OPS-12.1S
	The identified events shall be reported to the appropriate departments for timely assessment and remediation.	OPS-12.2S
High	The CSP shall automatically monitor log data in order to identify security events that might lead to security incidents, in accordance with the logging and monitoring requirements.	OPS-12.1H
	The identified events shall be reported to the appropriate departments for timely assessment and remediation.	OPS-12.2H
	The CSP shall automatically monitor that event detection operates as intended on assets classified in the highest level of the asset classification catalogue (cf. AM-05.1H).	OPS-12.3H

A.9.12.3 Guidance requirements

- In OPS-12.2H, the objective is to automate monitoring on critical assets, so the “highest level” should not be too restrictive.

A.9.13 OPS-13 Logging and Monitoring – Access, Storage and Deletion

A.9.13.1 Objective

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

A.9.13.2 Requirements

Basic	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation.	OPS-13.1B
	The communication between the assets to be logged and the logging servers shall be authenticated and protected in integrity and confidentiality whenever possible.	OPS-13.2B
	Log data shall be deleted when it is no longer required for the purpose for which they were collected.	OPS-13.3B
Substantial	The CSP shall store all log data in an integrity-protected and aggregated form that allow its centralized evaluation.	OPS-13.1S

	The communication between the assets to be logged and the logging servers shall be authenticated, encrypted using state-of-the-art encryption.	OPS-13.2S
	When encryption is not feasible, the communications shall be accessible only by authorised personnel.	OPS-13.4S
	The CSP shall implement technically supported procedures to fulfil requirements related to log data access, storage and deletion restrictions, including access only for authorised users and systems and the enforcement of data retention periods.	OPS-13.5S
	The CSP shall provide CSCs, upon request, access to customer-specific logging through an API.	OPS-13.6S
	The logging shall comply with the CSP's protection requirements including logical or physical separation of log and customer data.	OPS-13.7S
	Log data shall be deleted when it is no longer required for the purpose for which they were collected.	OPS-13.3S
High	The CSP shall store all log data in an integrity-protected and aggregated form that allow its evaluation.	OPS-13.1H
	The CSP shall automatically monitor the aggregation and deletion of logging and monitoring data.	OPS-13.8H
	The communication between the assets to be logged and the logging servers shall be authenticated, encrypted using state-of-the-art encryption.	OPS-13.2H
	When encryption is not feasible, the communications shall be accessible only by authorised personnel.	OPS-13.4H
	The CSP shall implement technically supported procedures to fulfil requirements related to log data access, storage and deletion restrictions, including access only for authorised users and systems and the enforcement of data retention periods.	OPS-13.5H
	The CSP shall provide CSCs, upon request, access to customer-specific logging through an API.	OPS-13.6H
	The logging shall comply with the CSP's protection requirements, including logical or physical separation of log and customer data.	OPS-13.7H
	Log data shall be deleted when it is no longer required for the purpose for which they were collected.	OPS-13.3H

A.9.13.3 Guidance requirements

- The customer-specific logging may be specific "in terms of scope and duration of the retention period".
- Aggregation is intended here as a way to consolidate logging data from various origins

A.9.14 OPS-14 Logging and Monitoring – Attribution

A.9.14.1 Objective

Log data can be unambiguously attributed to a CSC.

A.9.14.2 Requirements

Basic	The log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis during and following a security incident.	OPS-14.1B
Substantial	The log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis during and following a security incident.	OPS-14.1S
	The CSP shall make available interfaces to enable CSCs to conduct forensic analysis and perform backups related to their usage of the systems.	OPS-14.2S
High	The log data generated allows an unambiguous identification of user accesses at the CSC level to support analysis during and following a security incident.	OPS-14.1H
	The CSP shall make available interfaces to enable CSCs to conduct forensic analysis and perform backups related to their usage of the systems.	OPS-14.2H
		OPS-14.3H

In the context of an investigation of a security incident concerning a CSC, the CSP shall have the ability to provide to the CSC log data relevant and limited to the CSC's use of the cloud service.

A.9.14.3 Guidance requirements

-

A.9.15 OPS-15 Logging and Monitoring – Configuration

A.9.15.1 Objective

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

A.9.15.2 Requirements

Basic	The CSP shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility, with a strong authentication. Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01).	OPS-15.1B OPS-15.2B
Substantial	The CSP shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility, with a strong authentication. Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01).	OPS-15.1S OPS-15.2S
High	The CSP shall restrict to authorized users only the access to system components used for logging and monitoring under their responsibility, with a strong authentication. Changes to the logging and monitoring configuration are made in accordance with applicable policies (cf. CCM-01).	OPS-15.1S OPS-15.2S

A.9.15.3 Guidance requirements

- Define strong authentication, with a mention to multi-factor authentication as the reference when humans are involved, and cryptographic authentication between machines.
- Change of log settings, configuration or state is only possible through a documented change management process which considers contractual and CSC compliance – 'High'

A.9.16 OPS-16 Logging and Monitoring – Availability

A.9.16.1 Objective

Systems for logging and monitoring are themselves monitored for availability.

A.9.16.2 Requirements

Basic	The CSP shall monitor the system components for logging and monitoring under its responsibility. The CSP shall automatically report failures to the responsible departments for assessment and remediation.	OPS-16.1B OPS-16.2B
Substantial	The CSP shall monitor the system components for logging and monitoring under its responsibility.	OPS-16.1S

	The CSP shall automatically report failures to the responsible departments for assessment and remediation.	OPS-16.2S
High	The CSP shall monitor the system components for logging and monitoring under its responsibility.	OPS-16.1H
	The CSP shall automatically report failures to the responsible departments for assessment and remediation.	OPS-16.2H
	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.	OPS-16.3H

A.9.16.3 Guidance requirements

- Add guidance about failure tolerance of individual components

A.9.17 OPS-17 Managing Vulnerabilities, Malfunctions and Errors – Policies

A.9.17.1 Objective

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

A.9.17.2 Requirements

Basic	The CSP shall define 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.	OPS-17.1B
	The CSP shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities.	OPS-17.2B
Substantial	The CSP shall define 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 covering 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. 	OPS-17.1S
	The CSP shall use a scoring system for the assessment of vulnerabilities that includes at least “critical” and “high” classes of vulnerabilities.	OPS-17.2S
	The CSP shall mandate in its policies and procedures that “critical” vulnerabilities are to be immediately engaged after identification of the critical vulnerability even outside of the working day, and that work on “high” vulnerabilities shall begin within one working day, with a regular follow-up of the vulnerability until it has been remediated.	OPS-17.3S

High	<p>The CSP shall <u>define</u> and implement in accordance to ISP-02 policies and procedures with technical and organisational measures to ensure the timely identification and addressing of <u>vulnerabilities</u> in the <u>system components</u> used to provide the <u>cloud service</u>, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Regular identification of <u>vulnerabilities</u>; • Assessment of the severity of identified <u>vulnerabilities</u>; • Prioritisation and implementation of actions to promptly remediate or mitigate identified <u>vulnerabilities</u> 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 <u>vulnerabilities</u>. <p>The CSP shall use a scoring system for the assessment of <u>vulnerabilities</u> that includes at least "critical" and "high" classes of <u>vulnerabilities</u>.</p> <p>The CSP shall mandate in its policies and procedures that "critical" <u>vulnerabilities</u> are to be immediately engaged after identification of the critical <u>vulnerability</u>, even outside of the working day, and that work on "high" <u>vulnerabilities</u> shall begin within one working day, with a regular follow-up of the <u>vulnerability</u> until it has been remediated.</p> <p>The CSP based on its asset inventory (cf. AM-01), shall identify <u>vulnerabilities</u> of components accessing CSC data or components critical to providing <u>cloud service</u>.</p> <p>The CSP shall remediate as quickly as possible the <u>vulnerabilities</u> affecting these components, including those whose criticality has been assessed lower than "high" by the component vendor.</p>	<p>OPS-17.1H</p> <p>OPS-17.2H</p> <p>OPS-17.3H</p> <p>OPS-17.4H</p> <p>OPS-17.5H</p>
------	--	--

A.9.17.3 Guidance requirements

- The requirement stops short of requiring the use of CVSS, although the CSP is encouraged to use the latest version of CVSS. As a rule of thumb (for CVSS 3.0):
 - 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
- 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

A.9.18 OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Online Registers

A.9.18.1 Objective

Online registers are used to identify and publish known vulnerabilities.

A.9.18.2 Requirements

Basic	<p>The CSP shall contribute updates to an easily accessible online register of publicly known <u>vulnerabilities</u>, that covers:</p> <ul style="list-style-type: none"> • The <u>cloud service</u>; • Assets provided by CSPs to CSCs, that require installation or operation by the CSC under their own responsibility. <p>The CSP shall determine when a <u>vulnerability</u> is notified to the CSC.</p> <p>The online register shall indicate at least the following information for every <u>vulnerability</u>:</p> <ul style="list-style-type: none"> • A presentation of the <u>vulnerability</u> following an industry-accepted scoring system; • A description of the remediation options for that <u>vulnerability</u>; • Information on the availability of updates or patches for that <u>vulnerability</u>; • 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. <p>The CSP shall consult regularly the online registers indicated by its subservice providers and suppliers, analyse the potential impact of the published <u>vulnerabilities</u> on the <u>cloud service</u>, and handle them according to the <u>vulnerability handling process</u> (cf. OPS-17).</p>	<p>OPS-18.1B</p> <p>OPS-18.2B</p> <p>OPS-18.3B</p> <p>OPS-18.4B</p>
Substantial	<p>The CSP shall contribute at least daily updates to an easily accessible online register of publicly known <u>vulnerabilities</u>, that covers:</p>	OPS-18.1S

	<ul style="list-style-type: none"> • The cloud service; • Assets provided by CSPs to CSCs, that require installation or operation by the CSC under their own responsibility. <p>The CSP shall determine when a vulnerability is notified to the CSC. OPS-18.2S</p> <p>The online register shall indicate at least the following information for every vulnerability: OPS-18.3S</p> <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. <p>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 CSCs. OPS-18.5S</p> <p>The CSP shall consult at least daily 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). OPS-18.4S</p>	
High	<p>The CSP shall contribute at least daily updates to an easily accessible online register of publicly known vulnerabilities, that covers: OPS-18.1H</p> <ul style="list-style-type: none"> • The cloud service; • Assets provided by CSPs to CSCs, that require installation or operation by the CSC under their own responsibility. <p>The CSP shall determine when a vulnerability is notified to the CSC. OPS-18.2H</p> <p>The online register shall indicate at least the following information for every vulnerability: OPS-18.3H</p> <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. <p>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 CSCs. OPS-18.5H</p> <p>The CSP shall consult at least daily 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). OPS-18.4H</p> <p>The CSP shall provide and promote, where appropriate, automatic update mechanisms for 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. OPS-18.6H</p>	

A.9.18.3 Guidance requirements

- Guidance is needed to explain what information needs to be made public, and in particular what information needs to be shared publicly (through this requirement) and with CABs (through the scheme)
- The Common Vulnerability Scoring System (CVSS) should be used (make sure to sync with OPS requirements)
- In OPS-18.7H, it should be possible to perform updates automatically (without interaction from the user) and to perform the updates only after explicit approval from the user, if required by the user.
- About OPS-18.4H, there should be a reminder that the scheme actually requires all online registers that may affect the certified cloud service to be made available to customers.

A.9.19 OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Vulnerability Identification

A.9.19.1 Objective

Tests are performed on a regular basis to identify vulnerabilities.

A.9.19.2 Requirements

Basic	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).	OPS-19.1B
Substantial	The CSP shall perform at least monthly 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).	OPS-19.1S
	The CSP shall have penetration tests carried out by qualified 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 assessment.	OPS-19.2S
	The CSP shall perform such penetration tests at least annually, and in case of significant changes to the cloud service.	OPS-19.3S
	The CSP shall assess the penetration test findings and handle each identified vulnerability according to defined policies and procedures (cf. OPS-18).	OPS-19.4S
	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 service.	OPS-19.5S
	The CSP shall correlate the possible exploits of discovered vulnerabilities with previous security incidents to identify if the vulnerability may have been exploited before its discovery.	OPS-19.6S
High	The CSP shall perform at least monthly 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).	OPS-19.1H
	The CSP shall perform a threat and vulnerability analysis, including in its scope the system components relevant to the provision of the cloud service in the area of responsibility of the CSP, based on reviews of the architecture and configuration of these system components, and of the CSP's source code, and on the performance of penetration tests by a qualified and independent team, including personnel and external service providers, according to a documented test methodology.	OPS-19.2H
	The CSP shall plan the activities of the threat and vulnerability analysis, including system component reviews and penetration testing, in a multi-annual work programme.	OPS-19.7H
	The CSP shall review this threat and vulnerability analysis at least annually, and in case of significant changes to the cloud service, including the performance of reviews and penetration tests on system components, as deemed necessary.	OPS-19.3H
	The CSP shall assess the findings from the threat and vulnerability analysis and handle each identified vulnerability according to defined policies and procedures (cf. OPS-18).	OPS-19.4H
	The CSP shall perform a root cause analysis on the vulnerabilities discovered during the threat and vulnerability analysis in order to assess to which extent similar vulnerabilities may be present in the cloud service.	OPS-19.5H
	The CSP shall correlate the possible exploits of discovered vulnerabilities with previous security incidents to identify if the vulnerability may have been exploited before its discovery.	OPS-19.6H

A.9.19.3 Guidance requirements

- Guidance should define the test on publicly known vulnerabilities, with references to tools such as vulnerability scanners and security analysis tools (for analysing source code and dependencies)
- Define the notion of "independence" of the pen testers in the guidance
- Introduce black-box testing for Substantial and White-Grey box testing for High
- A specific guidance for auditors should be defined to provide additional details about the evaluation activities to be performed.
- The guidance should mention some ways to verify the competences of personnel in charge of performing pen tests.
- Additional guidance for the CSP will be provided regarding the threat and vulnerability analysis, including guidance on the initial steps (the identification of vulnerabilities and threats that will guide the reviews and pen tests)
- Among the "system components relevant to the provision of the cloud service in the area of responsibility of the CSP", the configuration review by the CSP should consider
 - all servers and networks included in the perimeter of the service (in particular for infrastructure capabilities)
 - the virtualized resources and basic software (OS, middleware, databases, ...) (in particular for platform and application capabilities)

- The source code review by the CSP should consider at least (when developed by the CSP)
 - the security functions provided to applications or users (e.g., IAM, session management, partitioning management)
 - the user interfaces, and in particular the administration interfaces.
- The reviews, and in particular the configuration reviews, should use sampling
- The reviews should be based on manual reviews by experts or a combination of such reviews with the use of automated tools.
- The reviews (noun) are security-related activities, whereas the act of reviewing mentioned in OPS-19.3H is about updating with up-to-date information
- The penetration tests of the CSP should be guided by the identified vulnerabilities and threats, and by the results of the reviews, with a specific focus on the most accessible components, such as user and administration interfaces
- The threat and vulnerability analysis should be made available to the auditor, including the results of the penetration testing, to allow them to get a full understanding of the activities undertaken.

A.9.20 OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures

A.9.20.1 Objective

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

A.9.20.2 Requirements

Basic	The CSP shall regularly measure, analyse and assess the procedures with which vulnerabilities and security incidents related to the cloud service are handled to verify their continued suitability, appropriateness and effectiveness.	OPS-20.1B
Substantial	The CSP shall regularly measure, analyse and assess the procedures with which vulnerabilities and security incidents related to the cloud service are handled to verify their continued suitability, appropriateness and effectiveness.	OPS-20.1S
	The CSP shall organise a quarterly review of the results of this assessment by accountable departments to initiate continuous improvement actions and verify their effectiveness.	OPS-20.2S
	This quarterly review shall be documented.	OPS-20.3S
High	The CSP shall regularly measure, analyse and assess the procedures with which vulnerabilities and security incidents related to the cloud service are handled to verify their continued suitability, appropriateness and effectiveness.	OPS-20.1H
	The CSP shall organise a quarterly review of the results of this assessment by accountable departments to initiate continuous improvement actions and verify their effectiveness.	OPS-20.2H
	This quarterly review shall be documented.	OPS-20.3H

A.9.20.3 Guidance requirements

-

A.9.21 OPS-21 Managing Vulnerabilities, Malfunctions and Errors – System Hardening

A.9.21.1 Objective

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

A.9.21.2 Requirements

Basic	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards.	OPS-21.1B
	The hardening requirements for each system component shall be documented.	OPS-21.2B
Substantial	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards.	OPS-21.1S
	The hardening requirements for each system component shall be documented.	OPS-21.2S
High	The CSP shall harden all the system components under its responsibility that are used to provide the cloud service, according to accepted industry standards.	OPS-21.1H
	The CSP shall automatically monitor these system components for conformity with hardening requirements.	OPS-21.3H
	The hardening requirements for each system component shall be documented.	OPS-21.2H

A.9.21.3 Guidance requirements

- 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.
- The CSP should annually conduct a documented full review of components to identify elements which erroneously have been left unhardened (Substantial)
- Provide examples of industry-accepted standards (typically, recommendations from manufacturers/vendors or user communities)

26.1.1 OPS-22 Separation of Datasets in the Cloud Infrastructure

A.9.21.4 Objective

The datasets from different CSCs are segregated to ensure their confidentiality and integrity.

A.9.21.5 Requirements

Basic	The CSP shall segregate from other CSCs the data stored and processed on shared virtual and physical resources on behalf of a CSC to ensure the confidentiality and integrity of this data.	OPS-22.1B
Substantial	The CSP shall segregate from other CSCs the data stored and processed on shared virtual and physical resources on behalf of a CSC to ensure the confidentiality and integrity of this data, according to the results of a risk assessment (cf. RM-01) and following policies on cryptography (cf. CKM-01) when relevant.	OPS-22.1S
High	The CSP shall segregate from other CSCs the data stored and processed on shared virtual and physical resources on behalf of a CSC to ensure the confidentiality and integrity of this data, according to the results of a risk assessment (cf. RM-01) and following policies on cryptography (cf. CKM-01) when relevant.	OPS-22.1H

A.9.21.6 Guidance requirements

- There are many ways to achieve segregation, virtually or physically, or even with table-level encryption in databases

A.10 IDENTITY, AUTHENTICATION AND ACCESS CONTROL MANAGEMENT

LIMIT ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES.

Term	Definition
emergency account	an account to be used when other accounts or authentication means are not available
role based access control	security technique for authentication that authorizes operations or allows access to resources based upon the user's identity and his/her relationship to other users and entities EXAMPLE 1: A teacher has read/write access to the grades for his/her students (role: "the teacher of the student"), but no access to other students' grades EXAMPLE 2: A principal has read-only access to the grades of all of his/her teachers' students (role: "the principal of the teachers of the students"), but the principal is not permitted to change any grades [SOURCE: From ISO/IEC 20944-1:2013(en), 3.21.20.2]
access right	permission for a subject to access a particular asset for a specific type of operation [Source: ISO/IEC 2382:2015, 2126298]
credential	representation of an identity Note 1 to entry: A credential is typically made to facilitate data authentication of the identity information in the identity it represents. Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid. EXAMPLE: A credential can be a username, a username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc. [SOURCE: From ISO/IEC 24760-1:2011, 3.3.5]

A.10.1 IAM-01 Policies for Access Control to Information

A.10.1.1 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.

A.10.1.2 Requirements

Basic	<p>The CSP shall <u>define role and rights policies and procedures</u> for controlling access to information resources, according to ISP-02 and based on the business and security <u>requirements</u> of the CSP, in which at least the following aspects are covered:</p> <ul style="list-style-type: none"> Parameters to be considered for making <u>access control decisions</u>; Granting and modifying <u>access rights</u> based on the "least-privilege" principle and on the "need-to-know" principle; Segregation of duties between managing, approving and assigning <u>access rights</u>; Dedicated rules for users with privileged access; <u>Requirements</u> for the <u>approval</u> and documentation of the management of <u>access rights</u>. <p>The CSP shall link the <u>access control policy</u> defined in IAM-01.1 with the physical <u>access control policy</u> defined in PS-02.1, to guarantee that the access to the premises where information is located is also controlled.</p>	<p>IAM-01.1B</p> <p>IAM-01.2B</p>
-------	--	-----------------------------------

Substantial	<p>The CSP shall define role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on role-based access control and based on the business and security requirements of the CSP, in which at least the following aspects are covered:</p> <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. <p>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.</p>	IAM-01.1S
High	<p>The CSP shall define role and rights policies and procedures for controlling access to information resources, according to ISP-02 and based on role-based access control and based on the business and security requirements of the CSP, in which at least the following aspects are covered:</p> <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. <p>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.</p> <p>The CSP shall document any potential conflicts between access rights, for segregation of duties or other reasons.</p> <p>The CSP shall enforce that these conflicts of access rights do not occur.</p>	IAM-01.2S IAM-01.1H IAM-01.2H IAM-01.3H IAM-01.4H

A.10.1.3 *Guidance requirements*

- The incompatibilities between access rights would mostly be based on role-based access, where two roles cannot be assigned to a same person (e.g., issuing a request and approving the request)

A.10.2 IAM-02 Management of Identities

A.10.2.1 Objective

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

A.10.2.2 Requirements

Basic	<p>The CSP shall define policies for managing identities, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> Parameters to be considered for making access control decisions; Assignment of unique usernames; Definition of the different types of identities supported, and assignment of access control parameters and roles to be considered for each type; Events and periods of inactivity leading to disabling and removing identities; Specific measures for the management of identities used infrequently for emergency recovery and similar scenarios. <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to a single person and associated access rights to personnel that</p>	<p>IAM-02.1B</p> <p>IAM-02.2B</p>
-------	---	-----------------------------------

	<p>comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to multiple persons and associated access rights that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to non-human entities and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall be able to provide, for a given identity, whether it falls under the responsibility of the CSP or of the CSC, and based on contractual terms for shared responsibility, the list of the access rights currently granted to that identity.</p>	<p>IAM-02.3B</p> <p>IAM-02.4B</p> <p>IAM-02.5B</p>
Substantial	<p>The CSP shall define policies for managing identities, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> Parameters to be considered for making access control decisions; Assignment of unique usernames; Definition of the different types of identities supported, and assignment of access control parameters and roles to be considered for each type; Events and periods of inactivity leading to disabling and removing identities. Specific measures for the management of identities used infrequently for emergency recovery and similar scenarios. <p>The CSP shall extend these policies for identities under their responsibility with the following aspects:</p> <ul style="list-style-type: none"> Segregation of duties between managing, approving and assigning access rights to accounts; Regular review of assigned accounts and associated access rights; Measures to be taken in the event of potential identity compromise, such as disabling or removing identities; Requirements for the approval and documentation of the management of identities. <p>The CSP shall extend these policies for identities under the responsibility of the CSCs with the following aspects:</p> <ul style="list-style-type: none"> Access control mechanisms available to CSCs; Access control parameters that the CSC is allowed to configure. <p>The CSP shall define and implement according to ISP-02 procedures for managing identities assigned to a single person and associated access rights to personnel that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to multiple persons and associated access rights that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing accounts associated to non-human entities and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights policies (cf. IAM-01) and with the policies for managing accounts.</p> <p>The CSP shall be able to provide, for a given identity, whether it falls under the responsibility of the CSP or of the CSC, and based on contractual terms for shared responsibility, the list of the access rights currently granted to that identity.</p> <p>The CSP shall offer CSCs a self-service mechanism with which they can independently manage the identities under their responsibility.</p>	<p>IAM-02.1S</p> <p>IAM-02.6S</p> <p>IAM-02.7S</p> <p>IAM-02.2S</p> <p>IAM-02.3S</p> <p>IAM-02.4S</p> <p>IAM-02.5S</p> <p>IAM-02.8S</p>
High	<p>The CSP shall define policies for managing identities, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> Parameters to be considered for making access control decisions; Assignment of unique usernames; Definition of the different types of identities supported, and assignment of access control parameters and roles to be considered for each type; Events and periods of inactivity leading to disabling and removing identities. Specific measures for the management of identities used infrequently for emergency recovery and similar scenarios. <p>The CSP shall extend these policies for identities under their responsibility with the following aspects:</p> <ul style="list-style-type: none"> Segregation of duties between managing, approving and assigning access rights to identities; Regular review of assigned identities and associated access rights; Measures to be taken in the event of potential identity compromise, such as disabling or removing identities; 	<p>IAM-02.1H</p> <p>IAM-02.6H</p>

	<ul style="list-style-type: none"> Requirements for the approval and documentation of the management of identities. <p>The CSP shall extend these policies for identities under the responsibility of the CSCs with the following aspects:</p> <ul style="list-style-type: none"> Access control mechanisms available to CSCs; Access control parameters that the CSC is allowed to configure. <p>The CSP shall define and implement according to ISP-02 procedures for managing identities assigned to a single person and associated access rights to personnel that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to multiple persons and associated access rights that comply with the role and rights policies (cf. IAM-01) and with the policies for managing identities.</p> <p>The CSP shall define and implement according to ISP-02 procedures for managing identities associated to non-human entities and associated access rights to system components involved in the operation of the cloud service that comply with the role and rights policies (cf. IAM-01) and with the policies for managing accounts.</p> <p>The CSP shall be able to provide, for a given identity, whether it falls under the responsibility of the CSP or of the CSC, and based on contractual terms for shared responsibility, the list of the access rights currently granted to that identity.</p> <p>The CSP shall offer CSCs a self-service with which they can independently manage the identities under their responsibility.</p>	<p>IAM-02.7H</p> <p>IAM-02.2H</p> <p>IAM-02.3H</p> <p>IAM-02.4H</p> <p>IAM-02.5H</p> <p>IAM-02.8H</p>
--	--	---

A.10.2.3 Guidance requirements

- Provide a description of the three types of accounts (personal, non-personal shared, technical).
- Provide explanations about shared responsibilities
- At higher levels, the list of users and rights should be automatically maintained and immediately available upon request.

A.10.3 IAM-03 Disabling, re-enabling and removing identities

A.10.3.1 Objective

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

A.10.3.2 Requirements

Basic	<p>The CSP shall document and implement an automated mechanism to disable identities after a certain period of inactivity, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p> <p>The CSP shall document and implement an automated mechanism to disable identities after a certain number of failed authentication attempts, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p>	<p>IAM-03.1B</p> <p>IAM-03.2B</p>
Substantial	<p>The CSP shall document and implement an automated mechanism to disable identities after a certain period of inactivity, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p> <p>The CSP shall document and implement an automated mechanism to disable identities after a certain number of failed authentication attempts, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p> <p>The CSP shall document and implement a process to monitor stolen and compromised credentials and disable any pending identity for which an issue is identified, pending a review by an authorized person, and implement it on all identities under its responsibility to which privileged access rights are assigned.</p> <p>Such processes shall include an exception mechanism for use in cases where all of the accounts needed to manage the situation are potentially included in the breach.</p> <p>Approval from authorised personnel or system components is required to re-enable identities locked automatically.</p>	<p>IAM-03.1S</p> <p>IAM-03.2S</p> <p>IAM-03.3S</p> <p>IAM-03.4S</p> <p>IAM-03.5S</p>

	The CSP shall document and implement an automated mechanism to remove identities that have been disabled by another automatic mechanism after a certain period of inactivity, as defined in the policy of IAM-02.	IAM-03.6S
High	<p>The CSP shall document and implement an automated mechanism to disable identities after a certain period of inactivity, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p> <p>The CSP shall automatically monitor the application of this mechanism.</p> <p>The CSP shall document and implement an automated mechanism to disable identities after a certain number of failed authentication attempts, with exceptions for identities to be used in emergency recovery and similar scenarios, where extended periods of inactivity may be allowed.</p> <p>The CSP shall and automatically monitor the application of this mechanism.</p> <p>The CSP shall document and implement a process to monitor stolen and compromised credentials and lock any pending identity for which an issue is identified, pending a review by an authorized person, and implement it on all identities under its responsibility.</p> <p>Such processes shall include an exception mechanism for use in cases where all of the identities needed to manage the situation are potentially included in the breach.</p> <p>Approval from authorised personnel or system components is required to re-enable identities disabled automatically.</p> <p>The CSP shall document and implement an automated mechanism to remove identities that have been disabled by another automatic mechanism after a certain period of inactivity, as defined in the policy of IAM-02, and automatically monitor its application.</p> <p>The CSP shall automatically monitor the context of authentication attempts and flag suspicious events to the corresponding user or to authorized persons, as relevant.</p>	<p>IAM-03.1H</p> <p>IAM-03.7H</p> <p>IAM-03.2H</p> <p>IAM-03.8H</p> <p>IAM-03.3H</p> <p>IAM-03.4H</p> <p>IAM-03.5H</p> <p>IAM-03.6H</p> <p>IAM-03.9H</p>

A.10.3.3 Guidance requirements

- At level Basic, limits have to be defined, without constraints, but reasonable enough to convince the auditor of their efficiency.
- Include an explanation of “block” vs. “revoke” (revoke removes the account, so the creation process needs to be redone), including backup requirements for revocation to cover for long employee breaks.
- Add an explanation about detection of DDoS attacks based on abusing the locking mechanisms
- Add an explanation about how monitoring compromised credentials does not prevent the stealing, but is only intended to limit the exploitability of compromised credentials
- In IAM-3.6H, the “context” includes information like the location, time of the attempt, or even behaviour patterns such as typing patterns, to identify a potential fraudulent authentication attempt.

A.10.4 IAM-04 Management of Access Rights

A.10.4.1 Objective

Policies and procedures are defined for managing and controlling the assignment of access rights to accounts and to users.

A.10.4.2 Requirements

Basic	<p>The CSP shall document and implement procedures to grant, update, and revoke to an identity under its responsibility access rights to resources of the information system of the cloud service.</p> <p>These procedures shall be in conformity with the role and rights policies and with the policies for managing access rights</p> <p>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.</p>	<p>IAM-04.1B</p> <p>IAM-04.2B</p> <p>IAM-04.3B</p>
Substantial	The CSP shall document and implement procedures to grant, update, and revoke to an identity under its responsibility access rights to resources of the information system of the cloud service.	IAM-04.1S

	These procedures shall be in <u>conformity</u> with the <u>role</u> and rights <u>policies</u> and with the <u>policies</u> for managing access rights.	IAM-04.2S
	The <u>CSP</u> shall <u>document</u> and <u>implement</u> a <u>procedure</u> to timely update or revoke the <u>access rights</u> of an internal or external employee when the <u>role</u> and responsibilities of the employee change, <u>within 48 hours of the role change for privileged access rights</u> and <u>within 14 days for other access rights</u>	IAM-04.3S
	If the <u>CSP</u> defines identities to be used when the main authentication technology is not available, then the <u>CSP</u> shall define and enforce specific <u>requirements</u> related to these identities.	IAM-04.4S
	The <u>CSP</u> shall offer <u>CSCs</u> a self-service with which they can independently manage <u>access rights</u> for all identities under their responsibility.	IAM-04.5S
High	The <u>CSP</u> shall <u>document</u> and <u>implement</u> <u>procedures</u> to grant, update, and revoke to an account under its responsibility <u>access rights</u> to resources of the information system of the cloud service.	IAM-04.1H
	These procedures shall be in <u>conformity</u> with the <u>role</u> and rights <u>policies</u> and with the <u>policies</u> for managing access rights.	IAM-04.2H
	The <u>CSP</u> shall <u>document</u> and <u>implement</u> a <u>procedure</u> to timely update or revoke the <u>access rights</u> of an internal or external employee when the <u>role</u> and responsibilities of the employee change, <u>within 48 hours of the role change for privileged access rights</u> and <u>within 14 days for other access rights</u> .	IAM-04.3H
	If the <u>CSP</u> defines identities to be used when the main authentication technology is not available, then the <u>CSP</u> shall define and enforce specific <u>requirements</u> related to these identities.	IAM-04.4H
	The <u>CSP</u> shall offer <u>CSCs</u> a self-service with which they can independently manage <u>access rights</u> for all accounts under their responsibility.	IAM-04.5H
	The <u>CSP</u> shall <u>document</u> and <u>implement</u> a <u>procedure</u> to provide, for a given resource subject to <u>access control</u> , a report of all the identities that have access to it, whether they fall under the responsibility of the <u>CSP</u> or of a <u>CSC</u> and for every such identity the list of <u>access rights</u> currently granted to it.	IAM-04.6H
	The <u>access right</u> management procedures shall be applied without delay in a timely manner, rather than waiting for the next log-in.	IAM-04.7H

A.10.4.3 Guidance requirements

- The requirement on position change is only for internal changes, so the employee remains tied by the company's policies.
- The requirements on delays have been discussed and the constraint is realistic
- 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)

A.10.5 IAM-05 Regular Review of Access Rights

A.10.5.1 Objective

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

A.10.5.2 Requirements

Basic	The <u>CSP</u> shall <u>review</u> the <u>identities</u> under its responsibility and associated <u>access rights</u> at least once a year to ensure that they still correspond to the current needs.	IAM-05.1B
Substantial	The <u>CSP</u> shall <u>review</u> the identities under its responsibility and associated <u>access rights</u> at least once a year to ensure that they still correspond to the current needs.	IAM-05.1S
	The review shall be performed by authorised persons under the responsibility of the <u>authorised body</u> that has approved the <u>access rights policies</u>	IAM-05.2S
	The <u>CSP</u> handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating <u>access rights</u> .	IAM-05.3S
		IAM-05.4S

	The CSP shall provide CSCs with a tool that facilitates <u>reviewing</u> of the <u>access rights</u> of accounts under their responsibility.	
High	The CSP shall <u>review</u> the identities and associated <u>access rights</u> under its responsibility at least every six (6) months to ensure that they still correspond to the current needs.	IAM-05.1H
	The review shall be performed by authorised persons under the responsibility of the <u>authorised body</u> that has approved the <u>access rights</u> policies.	IAM-05.2H
	The CSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating <u>access rights</u> .	IAM-05.3H
	The CSP shall provide CSCs with a tool that facilitates <u>reviewing</u> of the <u>access rights</u> of accounts under their responsibility.	IAM-05.4H

A.10.5.3 Guidance requirements

- The delay for fixing deviations should be commensurate to the frequency of the review: 7 days is appropriate for biannual reviews, but a shorter delay may be better if reviews are more frequent

A.10.6 IAM-06 Privileged Access Rights

A.10.6.1 Objective

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

A.10.6.2 Requirements

Basic	<u>Identities</u> assigned to multiple persons under the responsibility of the CSP shall be assigned only to personnel.	IAM-06.1B
	The assigned identities shall follow IAM-05 requirements.	IAM-06.2B
	The CSP shall require strong authentication for accessing the administration interfaces used by the CSP.	IAM-06.3B
Substantial	Privileged <u>access rights</u> shall be tailored, limited in time according to a <u>risk assessment</u> and assigned as necessary for the execution of <u>tasks</u> (need-to-know principle).	IAM-06.4S
	<u>Activities</u> of identities with privileged <u>access rights</u> shall be logged in order to detect any misuse of privileged access or function in suspicious cases.	IAM-06.5S
	The logged information shall be automatically <u>monitored</u> for defined events that may indicate misuse.	IAM-06.6S
	The CSP shall <u>document</u> and <u>implement</u> a procedure that, upon detection of potential misuse by this <u>monitoring</u> , informs the responsible personnel so that they can promptly assess whether misuse has occurred and take corresponding action.	IAM-06.7S
	<u>Identities</u> assigned to multiple persons under the responsibility of the CSP shall be assigned only to personnel.	IAM-06.1S
	The assigned identities shall follow IAM-05 requirements.	IAM-06.2S
	The CSP shall require strong authentication for accessing the administration interfaces used by the CSP.	IAM-06.3S
High	Privileged <u>access rights</u> shall be tailored, limited in time according to a <u>risk assessment</u> and assigned as necessary for the execution of tasks (need-to-know principle).	IAM-06.4H
	<u>Activities</u> of identities with privileged <u>access rights</u> shall be logged in order to detect any misuse of privileged access or function in suspicious cases.	IAM-06.5H
	The logged information shall be automatically <u>monitored</u> for defined events that may indicate misuse.	IAM-06.6H
	The CSP shall document and implement a procedure that, upon detection of potential misuse by this <u>monitoring</u> , informs the responsible personnel so that they can promptly assess whether misuse has occurred and take corresponding action.	IAM-06.7H
	<u>Identities</u> assigned to multiple persons under the responsibility of the CSP shall be assigned only to <u>personnel</u> .	IAM-06.1H
	The assigned <u>identities</u> shall follow IAM-05 <u>requirements</u> .	IAM-06.2H

	The CSP shall review every three (3) months the list of personnel who are responsible for an identity assigned to a non-human entity within its scope of responsibility.	IAM-06.8H
	The CSP shall maintain an up-to-date inventory of the identities under its responsibility that have privileged access rights.	IAM-06.9H
	The CSP shall require strong authentication for accessing the administration interfaces used by the CSP and those offered to the CSCs.	IAM-06.3H

A.10.6.3 Guidance requirements

- Define the users who are excluded from privileged access rights
- The CSP should create and maintain a user privilege escalation detection process. – 'Substantial'
- Automation of the monitoring of privileged users activities is designed as a way to obtain a good balance between the coverage of the monitoring and its cost. At Substantial level, the implementation requirements may not be as strict as for typical "automated monitoring" requirements at High level.

A.10.7 IAM-07 Authentication Mechanisms

A.10.7.1 Objective

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

A.10.7.2 Requirements

Basic	The CSP shall define and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects:	IAM-07.1B
	<ul style="list-style-type: none"> • The selection of mechanisms suitable for every type of identity and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new identities; • 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. 	
	The access to all environments of the CSP shall be authenticated, including non-production environments.	IAM-07.2B
	All authentication mechanisms shall include a mechanism to block an account after a predefined number of unsuccessful attempts.	IAM-07.3B
Substantial	The CSP shall define and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects:	IAM-07.1S
	<ul style="list-style-type: none"> • The selection of mechanisms suitable for every type of identity and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new identities; • 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. 	
	The access to all environments of the CSP shall be authenticated, including non-production environments.	IAM-07.2S
	The access to all environments under the control of the CSP that contain CSC data associated to the cloud service, including the production environment of the CSP shall require strong authentication.	IAM-07.4S
	Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security.	IAM-07.5S
	For access to non-personal identities assigned to several persons, the CSP shall implement measures that require the users to be authenticated with the identity assigned to a single person before being able to access these identities associated to multiple persons.	IAM-07.6S

	All authentication mechanisms shall include a mechanism to disable an identity after a predefined number of unsuccessful attempts.	IAM-07.3S
	The CSP shall offer strong authentication methods to the CSC for use with the identities under their responsibility.	IAM-07.7S
	The CSP shall distribute credentials using additional security mechanisms to verify the identity of the recipient, validate the request and protect the credentials.	IAM-08.8S
High	<p>The CSP shall define and implement according to ISP-02 policies and procedures about authentication mechanisms, covering at least the following aspects:</p> <ul style="list-style-type: none"> • The selection of mechanisms suitable for every type of identity and each level of risk; • The protection of credentials used by the authentication mechanism; • The generation and distribution of credentials for new identities; • 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. <p>The access to all environments of the CSP shall be authenticated, including non-production environments.</p> <p>The access to all environments under the control of the CSP that contain CSC data associated to the cloud service, including the production environment of the CSP shall require strong authentication.</p> <p>Within an environment, user authentication shall be performed through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security.</p> <p>For access to non-personal identities shared between several persons, the CSP shall implement measures that require the users to be authenticated with the identity assigned to a single person before being able to access these shared identities associated to multiple persons.</p> <p>All authentication mechanisms shall include a mechanism to disable an identity after a predefined number of unsuccessful attempts.</p> <p>The CSP shall offer strong authentication methods to the CSC for use with the identities under their responsibility.</p> <p>The CSP shall distribute credentials using additional security mechanisms to verify the identity of the recipient, validate the request and protect the credentials.</p>	<p>IAM-07.1H</p> <p>IAM-07.2H</p> <p>IAM-07.4H</p> <p>IAM-07.5H</p> <p>IAM-07.6H</p> <p>IAM-07.3H</p> <p>IAM-07.7H</p> <p>IAM-07.8H</p>

A.10.7.3 Guidance requirements

- Define the notion of strong authentication, maybe referring to external documentation

A.10.8 IAM-08 Protection and Strength of Credentials

A.10.8.1 Objective

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

A.10.8.2 Requirements

Basic	<p>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:</p> <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; • Confidentiality of personal (or shared) authentication and non-sharing of credentials. <p>Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01) except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.</p>	<p>IAM-08.1B</p> <p>IAM-08.2B</p>
-------	--	-----------------------------------

	In the latter case stored passwords shall be protected, where feasible using a cryptographically strong mechanism.	IAM-08.3B
	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	IAM-08.4B
Substantial	<p>The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of <u>credentials</u>, including at least:</p> <ul style="list-style-type: none"> • Non-reuse of <u>credentials</u>; • Trade-offs between entropy and ability to memorize; • Recommendations for renewal of passwords; • Rules on storage of passwords • Confidentiality of personal (or shared) authentication and non-sharing of <u>credentials</u>; • Recommendations on password managers • Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling <p>Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01) except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.</p> <p>In the latter case stored passwords shall be protected, where feasible using a cryptographically strong mechanism.</p> <p>If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.</p> <p>When creating <u>credentials</u>, compliance with policies is enforced automatically as far as technically possible.</p> <p>When a <u>credential</u> associated to an identity assigned to a single person is changed or renewed, the person associated to that account shall be notified.</p> <p>Any password reset procedure shall be valid for less than 48 hours.</p> <p>The password shall be changed by the user after the use of the reset procedure.</p> <p>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.</p>	<p>IAM-08.1S</p> <p>IAM-08.2S</p> <p>IAM-08.3S</p> <p>IAM-08.4S</p> <p>IAM-08.5S</p> <p>IAM-08.6S</p> <p>IAM-08.7S</p> <p>IAM-08.8S</p> <p>IAM-08.9S</p>
High	<p>The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of <u>credentials</u>, including at least:</p> <ul style="list-style-type: none"> • Non-reuse of <u>credentials</u>; • Trade-offs between entropy and ability to memorize; • Recommendations for renewal of passwords; • Rules on storage of passwords; • Confidentiality of personal (or shared) authentication and non-sharing of <u>credentials</u>; • Recommendations on password managers • Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling <p>The CSP shall require users under its responsibility to whom authentication <u>credentials</u> are provided to acknowledge that they treat personal (or shared) authentication confidentially and will not share the <u>credentials</u> with other persons.</p> <p>Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01) except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.</p> <p>In the latter case stored passwords shall be protected, where feasible using a cryptographically strong mechanism.</p> <p>If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.</p> <p>When creating <u>credentials</u>, compliance with policies is enforced automatically as far as technically possible.</p> <p>When a <u>credential</u> associated to an identity assigned to a single person is changed or renewed, the person associated to that account shall be notified.</p> <p>Any password reset procedure shall be valid for less than 48 hours.</p> <p>The password shall be changed by the user after the use of the reset procedure..</p> <p>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.</p>	<p>IAM-08.1H</p> <p>IAM-08.10H</p> <p>IAM-08.2H</p> <p>IAM-08.3H</p> <p>IAM-08.4H</p> <p>IAM-08.5H</p> <p>IAM-08.6H</p> <p>IAM-08.7H</p> <p>IAM-08.8H</p> <p>IAM-08.9H</p>

A.10.8.3 Guidance requirements

- Define the notion of strong hashes, maybe referring to other chapters or to external documentation

A.10.9 IAM-09 General Access Restrictions

A.10.9.1 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.

A.10.9.2 Requirements

Basic	<p>The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems. IAM-09.1B</p> <p>The CSP shall implement suitable measures for partitioning between the CSCs IAM-09.2B</p>
Substantial	<p>The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems. IAM-09.1S</p> <p>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. IAM-09.3S</p> <p>The CSP shall implement suitable measures for partitioning between the CSCs. IAM-09.2S</p> <p>The CSP shall inform the CSC through contractual agreements, prior to offering its services, all instances where CSP access in a non-encrypted form to the CSC's CSC data processed, stored or transmitted in the cloud service may occur. IAM-09.4S</p> <p>The CSP shall timely inform a CSC whenever personnel of the CSP access to the CSC's CSC data processed, stored or transmitted in the cloud service without the prior consent of the CSC including at least: IAM-09.5S</p> <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. <p>If the CSP offers to its CSCs interfaces for administrators and for end users, these interfaces shall be separated. IAM-09.6S</p>
High	<p>The CSP shall implement sufficient partitioning measures between the information system providing the cloud service and its other information systems. IAM-09.1H</p> <p>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. IAM-09.3H</p> <p>The CSP shall separate the administration interfaces made available to CSCs from those made available to its internal and external employees and in particular: IAM-09.7H</p> <ul style="list-style-type: none"> The identities under the responsibility of the CSP shall be managed using instances of tools and directories that are different from those used for the management of accounts under the responsibility of the CSCs; The administration interfaces made available to CSCs shall not allow for any connection from identities 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 identities under the responsibility of the CSC. <p>The CSP shall implement suitable measures for partitioning between the CSCs. IAM-09.2H</p> <p>The CSP may agree with the CSC, necessarily through contractual agreements, instances where CSP access in a non-encrypted form to the CSC's data processed, stored or transmitted in the cloud service may occur where requiring prior consent is not feasible (for example, where troubleshooting the service is necessary to ensure that the CSC's data remains confidential, available and its integrity preserved). IAM-09.4H</p> <p>The CSP shall require prior consent from a CSC before any access to the CSC's CSC data processed, stored or transmitted in the cloud service, with enforcement using technical means, and providing meaningful information, including at least: IAM-09.5H</p> <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.

If the CSP offers to its CSCs interfaces for administrators and for end users, these interfaces shall be separated.	IAM-09.6H
Before granting to an employee direct or indirect access to CSC data including in support operations, the CSP shall verify that the employee performing the action has passed an appropriate assessment or is supervised by an employee who has passed an appropriate assessment (cf. HR-02.1S).	IAM-09.8H
In the case of supervised access, the CSP shall ensure that: <ul style="list-style-type: none"> the access is performed using mechanisms that allow the supervising employee to authorize or deny individual actions, ask for explanations, in real time; the access rights are revoked at the end of the operation; the operations performed are logged as administrative actions. 	IAM-09.9H
In the case of supervised access, the CSP shall ensure that the supervision solution: <ul style="list-style-type: none"> includes the authentication the supervised employee and the device from which the supervised access is performed; logs the operations proposed by the supervised employee and the actions of the supervisor, including the operations denied by the supervisor; prevents information flows toward the supervised employee's device. 	IAM-09.10H

A.10.9.3 Guidance requirements

- Define the notion of partitioning and separation
- Provide examples of the "suitable means" mentioned in IAM-09.2
- The type of access described in IAM-09.5 should be treated as incident or data breach, if the CSC finds the reasoning unsatisfactory. – 'Substantial'
- The notion of "public network" needs to be defined, indicating that the use of VPNs or 0-trust, are not considered public. Also clarify that such accesses should be performed on specific hardware (admin laptops)
- The "separated" administration interfaces for CSPs and CSCs may be different instances of the same tool, each with their own configuration and access control
- Access to CSC data means access in non-encrypted form, or access in encrypted form with access to the decryption key
- Authorisation to access CSC data in specified circumstances can be included in the contractual agreements, which should be considered as "prior consent"

A.11 CRYPTOGRAPHY AND KEY MANAGEMENT

ENSURE APPROPRIATE AND EFFECTIVE USE OF CRYPTOGRAPHY TO PROTECT THE CONFIDENTIALITY, AUTHENTICITY OR INTEGRITY OF INFORMATION.

Term	Definition
state of the art	<p>developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience</p> <p>Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the “generally acknowledged state of the art”.</p> <p>[SOURCE: From ISO/IEC Guide 63:2019, 3.18]</p>
strong	<p>not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built</p> <p>[SOURCE: From ISO/IEC 19790:2012, 3.123]</p>
data in motion	<p>data being transferred from one location to another</p> <p>Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device).</p> <p>[SOURCE: From ISO/IEC 27040:2015(en), 3.8]</p>
data at rest	<p>data stored on stable non-volatile storage</p> <p>[SOURCE: From ISO/IEC 27040:2015(en), 3.6]</p>

A.11.1 CKM-01 Policies for the Use of Cryptography and Key Management

26.1.1.1 Objective

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

A.11.1.1 Requirements

Basic	<p>The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> • Usage of strong cryptographic mechanisms 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. 	CKM-01.1B
Substantial	<p>The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> • Usage of strong cryptographic mechanisms and secure network protocols, corresponding to the state-of-the-art; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; • Consideration of relevant legal and regulatory obligations and requirements. 	CKM-01.1S

	<ul style="list-style-type: none"> • 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 	
High	<p>The CSP shall define and implement policies with technical and organizational safeguards for cryptography and key management, according to ISP-02, in which at least the following aspects are described:</p> <ul style="list-style-type: none"> • Usage of strong cryptographic mechanisms and secure network protocols, corresponding to the state-of-the-art; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys; • Consideration of relevant legal and regulatory obligations and requirements. • 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 	CKM-01.1H

A.11.1.2 Guidance requirements

- Cryptographic mechanisms include at least encryption/decryption, signature/verification, random number generation, hashing. (...)
- The notion of “strong cryptography” will be defined in the guidance
- The notion of “state-of-the-art” will be defined in a dedicated cryptography guidance, to be worked on with the ECCG. Note that the state of the art to be considered may not be the same at all levels. At level Substantial, state of the art may be mostly about using proper algorithms, whereas at High, it should include resistance against state-of-the-art crypto attacks.

A.11.2 CKM-02 Encryption of Data in motion

A.11.2.1 Objective

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

A.11.2.2 Requirements

Basic	<p>The CSP shall define and implement strong cryptographic mechanisms for the transmission of CSC data over public networks, in order to protect the confidentiality, integrity and authenticity of data.</p> <p>The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment including personnel authentication.</p>	<p>CKM-02.1B</p> <p>CKM-02.2B</p>
Substantial	<p>The CSP shall define and implement strong cryptographic mechanisms for the transmission of CSC data over public networks, in order to protect the confidentiality, integrity and authenticity of data.</p> <p>The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including personnel authentication.</p>	<p>CKM-02.1S</p> <p>CKM-02.2S</p>
High	<p>The CSP shall define and implement strong cryptographic mechanisms for the transmission of all data over public networks, in order to protect the confidentiality, integrity and authenticity of data.</p> <p>The CSP shall use strong cryptographic mechanisms to protect the communication during remote access to the production environment, including employee authentication.</p>	<p>CKM-02.1H</p> <p>CKM-02.2H</p>

A.11.2.3 Guidance requirements

- The notion of “strong cryptography” will be defined in the guidance

A.11.3 CKM-03 Encryption of Data at Rest

A.11.3.1 Objective

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

A.11.3.2 Requirements

Basic	The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	CKM-03.1B
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	CKM-03.2B
Substantial	The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	CKM-03.1S
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	CKM-03.2S
	The private and secret keys used for encryption of sensitive CSC data shall be known only to the CSC in accordance with applicable legal and regulatory obligations and requirements, with the possibility of exceptions.	CKM-03.3S
	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be established in accordance with applicable legal and regulatory obligations and requirements and contractually agreed with the CSC.	CKM-03.4S
High	The CSP shall define and implement procedures and technical safeguards to protect the confidentiality of CSC data during storage, according to ISP-02.	CKM-02.1H
	The CSP shall notify CSCs of updates of these procedures and technical safeguards and to changes in the storage of CSC data that may affect the confidentiality of the data.	CKM-03.2H
	The procedures for the use of private and secret keys, including a specific procedure for any exceptions, shall be established in accordance with applicable legal and regulatory obligations and requirements and contractually agreed with the CSC.	CKM-03.3H
		CKM-03.4H

A.11.3.3 Guidance requirements

- The notion of “sensitive data” (requiring specific encryption with a key controlled by the CSC) is not necessarily known to the CSP:
 - a) An Application Provider should know which data is sensitive (e.g., personal data), and take appropriate actions.
 - b) An Infrastructure provider does not necessarily know which data is sensitive, but they should provide a generic mechanism where the CSC can store the data it believes is sensitive.

A.11.4 CKM-04 Secure Key Management

A.11.4.1 Objective

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

A.11.4.2 Requirements

Basic	<p>Procedures and technical safeguards for secure key management in the area of responsibility of the CSP shall include at least the following aspects:</p> <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; 	CKM-04.1B
-------	--	-----------

	<ul style="list-style-type: none"> • 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; 	
Substantial	<p>Procedures and technical safeguards for secure key management in the area of responsibility of the <u>CSP</u> shall include at least the following aspects:</p> <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; <p>For the secure storage of keys, the key management system shall be separated from the application and middleware levels.</p> <p>If pre-shared keys are used, the specific provisions relating to the secure use of this <u>procedure</u> shall be specified separately.</p>	<p>CKM-04.1S</p> <p>CKM-04.2S</p> <p>CKM-02.3S</p>
High	<p>Procedures and technical safeguards for secure key management in the area of responsibility of the <u>CSP</u> shall include at least the following aspects:</p> <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; <p>For the secure storage of keys, the key management system shall be separated from the application and middleware levels.</p> <p>For the secure storage of keys and other secrets used for the administration tasks, the <u>CSP</u> shall use a suitable software or hardware security container.</p> <p>If pre-shared keys are used, the specific provisions relating to the secure use of this <u>procedure</u> shall be specified separately.</p>	<p>CKM-04.1H</p> <p>CKM-04.2H</p> <p>CKM-02.4H</p> <p>CKM-02.3H</p>

A.11.4.3 Guidance requirements

- Provide explanations on suitable security containers and separation between application and middleware levels

A.12 COMMUNICATION SECURITY

ENSURE THE PROTECTION OF INFORMATION IN NETWORKS AND THE CORRESPONDING INFORMATION PROCESSING SYSTEMS.

Term	Definition
security zone	area of a network in which limited data exchange with areas outside is allowed [SOURCE: From ISO/TR 11636:2009(en), 2.13]
demilitarized zone DMZ	perimeter network (also known as a screened sub-net) inserted as a “neutral zone” between networks [SOURCE: From ISO/IEC 27033-1:2015(en), 3.8]
virtual local area network VLAN	independent network created from a logical point of view within a physical network [SOURCE: From ISO/IEC 27033-1:2015(en), 3.41]
tunnel	data path between networked devices which is established across an existing network infrastructure Note 1 to entry: Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits [SOURCE: From ISO/IEC 27033-1:2015(en), 3.40]

A.12.1 CS-01 Technical safeguards

A.12.1.1 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.

A.12.1.2 Requirements

Basic	The CSP shall define 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.	CS-01.1B
Substantial	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, and based on the results of a risk analysis carried out according to RM-01.	CS-01.1S
	The CSP shall feed into a SIEM (Security Information and Event Management) system, all data from these technical safeguards implemented so that automatic countermeasures regarding correlating security events are initiated.	CS-01.2S
High	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, and based on the results of a risk analysis carried out according to RM-01.	CS-01.1H
	The CSP shall implement technical safeguards to ensure that only authorized (physical or virtual) devices join its (physical or virtual) network.	CS-01.3H
	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 security events are initiated.	CS-01.2H
	The CSP shall use technologies for its technical safeguards that provide automated protection and prevention at multiple tiers (defence in depth) within the cloud service.	CS-01.4H

A.12.1.3 Guidance requirements

- From C5. “on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial- of-Service (DDoS) attacks”.
- Describe the requirement for High on multiple technologies, and how multiple technologies can be used
- Describe the various ways to “authorize” a device

A.12.2 CS-02 Security Requirements to Connect within the CSP’s Network

A.12.2.1 Objective

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

A.12.2.2 Requirements

Basic	<p>The CSP shall define and implement according to ISP-02 specific security <u>requirements</u> to connect within its network, including at least:</p> <ul style="list-style-type: none"> • when the <u>security zones</u> are to be separated and when the <u>CSCs</u> 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. 	CS-02.1B
Substantial	<p>The CSP shall define and implement according to ISP-02 specific security <u>requirements</u> to connect within its network, including at least:</p> <ul style="list-style-type: none"> • when the <u>security zones</u> are to be separated and when the <u>CSCs</u> 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. 	CS-02.1S
High	<p>The CSP shall define and implement according to ISP-02 specific security <u>requirements</u> to connect within its network, including at least:</p> <ul style="list-style-type: none"> • when the <u>security zones</u> are to be separated and when the <u>CSCs</u> 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. 	CS-02.1H

A.12.2.3 Guidance requirements

-

A.12.3 CS-03 Monitoring of Connections within the CSP’s Network

A.12.3.1 Objective

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

A.12.3.2 Requirements

Basic	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment .	CS-03.1B
	The CSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ , if applicable).	CS-03.2B
	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).	CS-03.3B
	The CSP shall review at specified intervals the business justification for using all services, protocols, and ports.	CS-03.4B
	This review shall also include the compensatory measures used for protocols that are considered insecure.	CS-03.5B
Substantial	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment according to RM-01.	CS-03.1S
	The CSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ , if applicable).	CS-03.2S
	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).	CS-03.3S
	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 .	CS-03.4S
	The CSP shall assess the risks of identified vulnerabilities in accordance with the risk management procedure (cf. RM-01).	CS-03.5S
	Follow-up measures shall be defined and tracked (cf. OPS-17).	CS-03.6S
High	The CSP shall protect all SIEM logs to avoid tampering.	CS-03.7S
	The CSP shall distinguish between trusted and untrusted networks, based on a risk assessment according to RM-01.	CS-03.1H
	The CSP shall separate trusted and untrusted networks into different security zones for internal and external network areas (and DMZ , if applicable).	CS-03.2H
	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).	CS-03.3H
	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 .	CS-03.4H
	The CSP shall assess the risks of identified vulnerabilities in accordance with the risk management procedure (cf. RM-01).	CS-03.5H
	Follow-up measures shall be defined and tracked (cf. OPS-17).	CS-03.6H
	The CSP shall protect all SIEM logs to avoid tampering.	CS-03.7H

A.12.3.3 Guidance requirements

•

A.12.4 CS-04 Networks for Administration

A.12.4.1 Objective

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

A.12.4.2 Requirements

Basic	The CSP shall define and implement separate networks for the system administration and the operation of management consoles.	CS-04.1B
-------	--	----------

	<p>The CSP shall logically or physically separate the networks for system administration from any other network. CS-04.2B</p> <p>The CSP shall segregate physically or logically the networks used to migrate or create virtual machines. CS-04.3B</p>	
Substantial	<p>The CSP shall define and implement separate networks for the system administration and the operation of management consoles. CS-04.1S</p> <p>The CSP shall logically or physically separate the networks for administration from any other network. CS-04.2S</p> <p>The CSP shall segregate physically or logically the networks used to migrate or create virtual machines. CS-04.3S</p>	
High	<p>The CSP shall define and implement separate networks for the system administration and the operation of management consoles. CS-04.1H</p> <p>The CSP shall logically or physically separate the networks for administration from any other network. CS-04.2H</p> <p>The CSP shall segregate physically or logically the networks used to migrate or create virtual machines. CS-04.3H</p> <p>When the administration networks are not physically segregated from other networks, the administration flows shall be protected using a strongly encrypted communication. CS-04.4H</p> <p>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. CS-04.5H</p>	

A.12.4.3 Guidance requirements

- In CS-04.5H, the application firewall may need to be complemented by other measures, depending on the interface.

A.12.5 CS-05 Traffic Separation in Shared Network Environments

A.12.5.1 Objective

The confidentiality and integrity of CSC data is protected by separation measures when communicated over shared networks.

A.12.5.2 Requirements

Basic	The CSP shall document and implement separation mechanisms at network level the data traffic of different CSCs. CS-05.1B	
Substantial	The CSP shall document and implement separation mechanisms at network level the data traffic of different CSCs. CS-05.1S	
High	<p>The CSP shall document and implement separation mechanisms at network level the data traffic of different CSCs. CS-05.1H</p> <p>When implementing infrastructure capabilities, the secure separation shall be ensured by physically separated networks or by strongly encrypted logical networks. CS-05.2H</p>	

A.12.5.3 Guidance requirements

- Separation mechanisms need to be described.
- The notion of strong encryption will be defined in the guidance for the CKM category.

A.12.6 CS-06 Network Topology Documentation

A.12.6.1 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 occurrence of malfunctions.

A.12.6.2 Requirements

Basic	The CSP shall maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service.	CS-06.1B
	The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with external and public networks, and the geographical locations in which the CSC data is stored.	CS-06.2B
Substantial	The CSP shall maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service.	CS-06.1S
	The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with external and public networks, and the geographical locations in which the CSC data is stored.	CS-06.2S
	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.	CS-06.3S
	The CSP shall perform a full review of the network topology documentation at least once a year.	CS-06.4S
High	The CSP shall maintain up-to-date all documentation of the logical structure of the network used to provision or operate the cloud service.	CS-06.1H
	The documentation shall cover, at least, how the subnets are allocated, how the network is zoned and segmented, how it connects with external and public networks, and the geographical locations in which the CSC data is stored.	CS-06.2H
	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.	CS-06.3H
	The CSP shall perform a full review of the network topology documentation at least once a year.	CS-06.4H

A.12.6.3 Guidance requirements

-

A.12.7 CS-07 Software-Defined Networking

A.12.7.1 Objective

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

A.12.7.2 Requirements

Basic	The CSP shall ensure the confidentiality of CSC data by suitable procedures when offering functions to CSCs for software-defined networking (SDN).	CS-07.1B
	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features.	CS-07.2B
Substantial	The CSP shall ensure the confidentiality of CSC data by suitable procedures when offering functions to CSCs for software-defined networking (SDN).	CS-07.1S
	The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features.	CS-07.2S

	The CSP shall ensure that the configuration of networks matches network security policies regardless of the means used to create the configuration.	CS-07.3S
High	The CSP shall ensure the confidentiality of CSC data by suitable procedures when offering functions to CSCs for software-defined networking (SDN). The CSP shall validate the functionality of the SDN functions before providing new SDN features to CSCs or modifying existing SDN features. The CSP shall ensure that the configuration of networks matches network security policies regardless of the means used to create the configuration.	CS-07.1H CS-07.2H CS-07.3H

A.12.7.3 Guidance requirements

- The Basic requirements may sound strong, but this is only for Infrastructure

A.12.8 CS-08 Data Transmission Policies

A.12.8.1 Objective

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

A.12.8.2 Requirements

Basic	The CSP shall define 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.	CS-08.1B
Substantial	The CSP shall define 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, and including references to the classification of assets (cf. AM-05).	CS-08.1S
High	The CSP shall define 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, and including references to the classification of assets (cf. AM-05).	CS-08.1S

A.12.8.3 Guidance requirements

-

A.13 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 CSP.

A.13.1 PI-01 Documentation and Security of Input and Output Interfaces

A.13.1.1 Objective

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

A.13.1.2 Requirements

Basic	Inbound and outbound interfaces that are made accessible for use by <u>cloud services</u> from other <u>CSPs</u> or <u>CSCs</u> ' IT systems shall be documented.	PI-01.1B
	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.	PI-01.2B
	Communication on these interfaces shall use commonly supported communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements, and the adequate authentication of the user.	PI-01.3B
	Communication over untrusted networks shall be protected in confidentiality, integrity and authenticity according to CKM-02.	PI-01.4B
Substantial	Inbound and outbound interfaces that are made accessible for use by <u>cloud services</u> from other <u>CSPs</u> or <u>CSCs</u> ' IT systems shall be documented.	PI-01.1S
	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.	PI-01.2S
	Communication on these interfaces shall use commonly supported communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements, and the adequate authentication of the user.	PI-01.3S
	Communication over untrusted networks shall be protected in confidentiality, integrity and authenticity according to CKM-02.	PI-01.4S
High	Inbound and outbound interfaces that are made accessible for use by <u>cloud services</u> from other <u>CSPs</u> or <u>CSCs</u> ' IT systems shall be documented.	PI-01.1H
	The interfaces shall be clearly documented for subject matter experts to understand how they can be used to retrieve the data.	PI-01.2H
	Communication on these interfaces shall use commonly supported communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements, and the adequate authentication of the user.	PI-01.3H
	Communication over untrusted networks shall be protected in confidentiality, integrity and authenticity according to CKM-02.	PI-01.4H
	The CSP shall allow its <u>CSCs</u> to verify the interfaces provided (and their security) are adequate for its protection requirements before the start of the use of the <u>cloud service</u> , and each time the interfaces are changed.	PI-01.5H

A.13.1.3 Guidance requirements

- Include guidance about the means to verify the interfaces at level High
- The idea of "commonly supported" protocol is meant to avoid obstacles to migration by the CSP

A.13.2 PI-02 Contractual Agreements for the Provision of Data

A.13.2.1 Objective

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

A.13.2.2 Requirements

Basic	<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 CSC; • 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. 	PI-02.1B
Substantial	<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 CSC; • 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. <p>These definitions 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.</p>	PI-02.1S PI-02.2S
High	<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 CSC; • 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. <p>These definitions 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.</p> <p>The CSP shall identify, at least once a year, legal and regulatory requirements that may apply to these aspects and review the contractual agreements accordingly.</p>	PI-02.1S PI-02.2S PI-02.3S

A.13.2.3 Guidance requirements

- The legal and regulatory requirements also include relevant sectoral and regulatory requirements.

A.13.3 PI-03 Secure Deletion of Data

A.13.3.1 Objective

CSC data is securely deleted upon termination of the contract.

A.13.3.2 Requirements

Basic	The CSP shall implement procedures for deleting its CSCs' data upon termination of their contract in compliance with the contractual agreements between them.	PI-03.1B
	The CSC's data deletion shall include all CSC data, as well as related metadata and cloud service derived data, such as data stored in data backups in accordance with the CSP's data retention policy and except as required by a valid court order.	PI-03.2B
	At the end of the contract, the CSP shall delete the technical data concerning the CSC, except as required by a valid court order or as needed to fulfil known future financial and legal obligations.	PI-03.3B
Substantial	The CSP shall implement procedures for deleting its CSCs' data upon termination of their contract in compliance with the contractual agreements between them.	PI-03.1S
	The CSC's data deletion shall include all CSC data, as well as related metadata and cloud service derived data, such as data stored in data backups in accordance with the CSP's data retention policy and except as required by a valid court order.	PI-03.2S
	The CSC's data deletion procedures shall prevent recovery by state-of-the-art forensic means.	PI-03.4S
	The CSP shall document the deletion of the CSC's data, including metadata and cloud service derived data, in a way allowing the CSC to track the deletion of its data.	PI-03.5S
	At the end of the contract, the CSP shall delete the technical data concerning the CSC, except as required by a valid court order or as needed to fulfil known future financial and legal obligations.	PI-03.3S
High	The CSP shall implement procedures for deleting its CSCs' data upon termination of their contract in compliance with the contractual agreements between them.	PI-03.1H
	The CSC's data deletion shall include all CSC data, as well as related metadata and cloud service derived data, such as data stored in data backups, except as required by a valid court order.	PI-03.2H
	The CSP's data deletion procedures shall prevent recovery by state-of-the-art forensic means.	PI-03.4H
	The CSP shall document the deletion of the CSC's data, including metadata and cloud service derived data, in a way allowing the CSC to track the deletion of its data.	PI-03.5H
	At the end of the contract, the CSP shall delete the technical data concerning the CSC, except as required by a valid court order or as needed to fulfil known future financial and legal obligations.	PI-03.3H

A.13.3.3 Guidance requirements

- The CSP should provide some assurance on the execution of the data deletion to the CSC (for level High)
- From SecNumCloud, technical data include data concerning the client and unknown to them, such as "directory, certificates, access configuration". Also, clarify what minimal retention of data covers, for instance billing data.

A.14 CHANGE AND CONFIGURATION MANAGEMENT

ENSURE THAT CHANGES AND CONFIGURATION ACTIONS TO INFORMATION SYSTEMS GUARANTEE THE SECURITY OF THE DELIVERED CLOUD SERVICE.

Term	Definition
change management	process for recording, coordination, approval and monitoring of all changes [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.3]
configuration management	process for logging and monitoring of configuration items [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.5]
version control	establishment and maintenance of baselines and the identification and control of changes to baselines that make it possible to return to the previous baseline [SOURCE: From ISO/IEC/IEEE 24765:2017(en), 3.4546]

A.14.1 CCM-01 Policies for Changes to Information Systems

A.14.1.1 Objective

Policies and procedures are documented, communicated and implemented to control changes to information systems.

A.14.1.2 Requirements

Basic	The CSP shall define and implement policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02.	CCM-01.1B
Substantial	<p>The CSP shall define and implement policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02, covering at least the following aspects:</p> <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 CSCs 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; • Requirements for the implementation and documentation of emergency changes, which must comply with the same level of security as normal changes; and • Requirements for the handling of a change's unexpected effects, including corrective actions. 	CCM-01.1S
High	<p>The CSP shall define and implement policies and procedures for change management of the IT systems supporting the cloud service according to ISP-02, covering at least the following aspects:</p> <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; 	CCM-01.1H

- Requirements for the proper information of CSCs 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;
- Requirements for the implementation and documentation of emergency changes, which must comply with the same level of security as normal changes; and
- Requirements for the handling of a change's unexpected effects, including corrective actions.

A.14.1.3 Guidance requirements

•

A.14.2 CCM-02 Risk Assessment, Categorisation and Prioritisation of Changes

A.14.2.1 Objective

Changes are categorised and prioritised according to potential security effects.

A.14.2.2 Requirements

Basic	The CSP shall categorise and prioritise changes considering the potential security effects on the system components concerned that are used to provide the cloud service.	CCM-02.1B
Substantial	The CSP shall categorise and prioritise changes considering the potential security effects on the system components concerned that are used to provide the cloud service.	CCM-02.1S
	The categorisation and prioritisation of changes shall be based on a risk assessment performed in accordance with RM-01 with regard to potential effects on the system components concerned, that are used to provide the cloud service.	CCM-02.2S
	If the risk associated to a planned change is high, then appropriate mitigation measures shall be taken before deploying the change in the cloud service's production environment.	CCM-02.3S
High	The CSP shall categorise and prioritise changes considering the potential security effects on the system components concerned, that are used to provide the cloud service.	CCM-02.1H
	based on a risk assessment performed in accordance with RM-01 with regard to potential effects on the system components concerned, that are used to provide the cloud service.	CCM-02.2H
	If the risk associated to a planned change is high, then appropriate mitigation measures shall be taken before deploying the change in the cloud service's production environment.	CCM-02.3H
	In accordance with contractual agreements, the CSP shall submit to authorised bodies of the CSC meaningful information about the time, duration, type and scope of the change so that they can carry out their own risk assessment	CCM-02.4H
	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	CCM-02.5H

A.14.2.3 Guidance requirements

•

A.14.3 CCM-03 Testing Changes

A.14.3.1 Objective

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

A.14.3.2 Requirements

Basic	The CSP shall <u>test</u> proposed changes before deployment to the <u>production environment</u> .	CCM-03.1B
	Before using <u>CSC data</u> for tests, the CSP shall first obtain approval from <u>CSC</u> and anonymise <u>CSC data</u> .	CCM-03.2B
	The CSP shall guarantee the confidentiality of the data during the whole process.	CCM-03.3B
Substantial	The CSP shall <u>test</u> proposed changes before deployment to the <u>production environment</u> .	CCM-03.1S
	The <u>type and scope of the tests</u> shall correspond to the <u>risk assessment</u> (cf. CCM-02).	CCM-03.4S
	The tests shall be carried out by appropriately qualified <u>personnel</u> or by automated, <u>state-of-the-art test procedures</u> .	CCM-03.5S
	In accordance with contractual requirements, the CSP shall involve <u>CSCs</u> into the tests.	CCM-03.6S
	Before using <u>CSC data</u> for tests, the CSP shall first obtain approval from <u>CSC</u> and anonymise <u>CSC data</u> .	CCM-03.2S
	The CSP shall guarantee the confidentiality of the data during the whole process.	CCM-03.3S
	The CSP shall determine the severity of the errors and <u>vulnerabilities</u> identified in the tests that are relevant for the deployment decision according to defined <u>criteria</u> .	CCM-03.7S
	The CSP shall initiate actions for timely remediation or mitigation.	CCM-03.8S
High	The CSP shall <u>test</u> proposed changes before deployment to the <u>production environment</u> .	CCM-03.1H
	The <u>type and scope of the tests</u> shall correspond to the <u>risk assessment</u> (cf. CCM-02).	CCM-03.4S
	The tests shall be carried out by appropriately qualified <u>personnel</u> or by automated, <u>state-of-the-art test procedures</u> .	CCM-03.5S
	The <u>tests performed on a change before its deployment to the production environment</u> shall include tests on the service performed on a <u>pre-production environment</u> .	CCM-03.9H
	Before deploying changes on a <u>system component</u> , the CSP shall perform <u>testing on other functional components of the cloud service that depend on that system component</u> to verify the absence of undesirable effects.	CCM-03.10H
	In accordance with contractual requirements, the CSP shall involve <u>CSCs</u> into the tests.	CCM-03.6H
	The CSP shall <u>document and implement a procedure that ensures the integrity of the test data used in the pre-production environment</u> .	CCM-03.11H
	Before using <u>CSC data</u> for tests, the CSP shall first obtain approval from <u>CSC</u> and anonymise <u>CSC data</u> .	CCM-03.2H
	The CSP shall guarantee the confidentiality of the data during the whole process.	CCM-03.3H
	The CSP shall determine the severity of the errors and <u>vulnerabilities</u> identified in the tests that are relevant for the deployment decision according to defined <u>criteria</u> , and shall initiate actions for timely remediation or mitigation.	CCM-03.7H

A.14.3.3 Guidance requirements

- The “state-of-the-art” procedures will be defined in guidance
- CCM-3.6H refers to integration or regression testing

A.14.4 CCM-04 Approvals for Provision in the Production Environment

A.14.4.1 Objective

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

A.14.4.2 Requirements

Basic	The CSP shall approve any change to the <u>cloud service</u> , based on defined <u>criteria</u> , before they are made available to <u>CSCs</u> in the <u>production environment</u>	CCM-04.1B
-------	--	-----------

Substantial	The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment.	CCM-04.1S
High	The CSP shall approve any change to the cloud service, based on defined criteria and involving CSCs in the approval process according to contractual requirements, before they are made available to CSCs in the production environment.	CCM-04.1H
	The approval processes shall be automatically monitored.	CCM-04.2H

A.14.4.3 Guidance requirements

- The CSP's approval may be provided by authorised personnel of the CSP or by an automated procedure enforcing defined criteria.
- The existence of CCM-04.1S should be mentioned in the guidance for cloud customers

A.14.5 CCM-05 Performing and Logging Changes

A.14.5.1 Objective

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

A.14.5.2 Requirements

Basic	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	CCM-05.1B
	All changes to the cloud service in the production environment shall be logged	CCM-05.2B
	All changes to the cloud service in the production environment shall be traceable back to the individual or system component that initiated the change.	CCM-05.3B
Substantial	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.	CCM-05.1S
	All changes to the cloud service in the production environment shall be logged	CCM-05.2S
	All changes to the cloud service in the production environment shall be traceable back to the individual or system component that initiated the change.	CCM-05.3S
High	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.	CCM-05.1H
	The changes to the cloud service in the production environment shall be automatically monitored to enforce these roles and rights.	CCM-05.4H
	All changes to the cloud service in the production environment shall be logged.	CCM-05.2H
	All changes to the cloud service in the production environment shall be traceable back to the individual or system component that initiated the change.	CCM-05.3H

A.14.5.3 Guidance requirements

-

A.14.6 CCM-06 Version Control

A.14.6.1 Objective

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

A.14.6.2 Requirements

Basic	The <u>CSP</u> shall implement version control <u>procedures</u> to track the dependencies of individual changes and to be able to restore affected <u>system components</u> back to their previous state as a result of errors or identified <u>vulnerabilities</u> .	CCM-06.1B
Substantial	The <u>CSP</u> shall implement version control <u>procedures</u> to track the dependencies of individual changes and to be able to restore affected <u>system components</u> back to their previous state as a result of errors or identified <u>vulnerabilities</u> .	CCM-06.1S
High	The <u>CSP</u> shall implement version control <u>procedures</u> to track the dependencies of individual changes and to be able to restore affected <u>system components</u> back to their previous state as a result of errors or identified <u>vulnerabilities</u> .	CCM-06.1H
	The version control <u>procedures</u> shall provide appropriate safeguards to ensure that the confidentiality, integrity and availability of <u>CSC data</u> is not compromised when <u>system components</u> are restored back to their previous state.	CCM-06.2H
	The <u>CSP</u> 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 <u>environment</u> , a similar environment such as was implemented on a given date.	CCM-06.3H
	The retention time for this history shall be at least the same as that for backups (cf. OPS-06).	CCM-06.4H

A.14.6.3 Guidance requirements

- Note that these requirements complement the OPS requirements on backup, which also include requirements on the security of customer data.
- 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.
- 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.15 DEVELOPMENT OF INFORMATION SYSTEMS

ENSURE INFORMATION SECURITY IN THE DEVELOPMENT CYCLE OF INFORMATION SYSTEMS

Term	Definition
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
outsourcing	acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's [SOURCE: From ISO/IEC 27036-1:2015, 3.6]

A.15.1 DEV-01 Policies for the Development and Procurement of Information Systems

A.15.1.1 Objective

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

A.15.1.2 Requirements

Basic	The <u>CSP</u> shall <u>define</u> and implement <u>policies</u> and <u>procedures</u> according to ISP-02 with technical and organisational measures for the secure development of the <u>cloud service</u> .	DEV-01.1B
	The <u>policies</u> and <u>procedures</u> for secure development shall consider <u>information security</u> from the earliest phases of design.	DEV-01.2B
Substantial	The <u>CSP</u> shall <u>define</u> and implement <u>policies</u> and <u>procedures</u> according to ISP-02 with technical and organisational measures for the secure development of the <u>cloud service</u> .	DEV-01.1S
	The <u>policies</u> and <u>procedures</u> for secure development shall consider <u>information security</u> from the earliest phases of design.	DEV-01.2S
	The <u>policies</u> and <u>procedures</u> for secure development they shall be based on established 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 (reducing the introduction of vulnerabilities in code). 	DEV-01.3S
	The <u>policies</u> and <u>procedures</u> for development shall include measures for the enforcement of specified standards and guidelines, including automated tools.	DEV-01.4S
High	The <u>CSP</u> shall <u>define</u> and implement <u>policies</u> and <u>procedures</u> according to ISP-02 with technical and organisational measures for the secure development of the <u>cloud service</u> .	DEV-01.1S
	The <u>policies</u> and <u>procedures</u> for secure development shall consider <u>information security</u> from the earliest phases of design.	DEV-01.2S

	<p>The policies and procedures for secure development shall be based on established standards and methods with regard to the following aspects:</p> <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 (reducing the introduction of <u>vulnerabilities</u> in code). 	DEV-01.3S
	<p>The policies and procedures for development shall include measures for the enforcement of specified standards and guidelines, including automated tools.</p>	DEV-01.4S

A.15.1.3 Guidance requirements

- Development activities must be understood widely, covering the production of software, as well as the production of configuration files, hypertext, and any material that can influence the provision of the service
- 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
- The software provision can be carried out, e.g. by Continuous Delivery methods
- Define what “established methods” cover, and in particular the fact that they may be private methods, as long as there is a history of scrutiny and usage (i.e., it is not a new method)

A.15.2 DEV-02 Development Supply Chain Security

A.15.2.1 Objective

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

A.15.2.2 Requirements

Basic	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its <u>cloud service</u> .	DEV-02.1B
Substantial	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its <u>cloud service</u> .	DEV-02.1S
	The CSP shall <u>define and implement policies and procedures</u> according to ISP-02 for the use of commercial and open source software.	DEV-02.2S
	The CSP shall retrieve software only from trusted sources.	DEV-02.3S
	The CSP shall verify authenticity of retrieved software when possible.	DEV-02.4S
High	The CSP shall maintain a list of dependencies to hardware and software products used in the development of its <u>cloud service</u> .	DEV-02.1H
	The CSP shall <u>define and implement policies and procedures</u> according to ISP-02 for the use of commercial and open source software.	DEV-02.2H
	The CSP shall retrieve software only from trusted sources.	DEV-02.3H
	The CSP shall verify authenticity of retrieved software when possible.	DEV-02.4H
	In procurement for the development of the cloud service, the CSP shall perform a <u>risk assessment</u> in accordance to RM-01 for every <u>product</u> .	DEV-02.5H

A.15.2.3 Guidance requirements

- For its software components, the list of dependencies is often called Software Board of Materials (SBOM). Guidance is required to explain that only directly use components need to be documented, but that sufficient information needs to be available on these components (see PM category for details).
- Article 51, point (d) of the EUCSA requires the identification and documentation of known dependencies. Dependencies should include all software modules, libraries or APIs used, as well as development tools.
- The policy should cover the following aspects:
 - Restrictions on component age;
 - Restrictions on outdated and EOL/EOS components;

- Restrictions on components with known vulnerabilities;
- Restrictions on public repository usage;
- Restrictions on acceptable licenses;
- Component update requirements;
- Deny list of prohibited components and versions; and
- Acceptable community contribution guidelines.
- This list is inspired from the OWASP requirements on open source software [OWASP CA].
- For open source software, the requirements on origin checks may need to be adapted to the circumstances.
- The use of certified products may considerably simplify the implementation of this requirement, because of the security guarantees that such a certification can bring.

A.15.3 DEV-03 Secure Development Environment

A.15.3.1 Objective

The development environment takes information security in consideration.

A.15.3.2 Requirements

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

A.15.3.3 Guidance requirements

- Here, source code has to be considered in a wide definition, i.e., any content that may influence the provision of the service, including configuration files, etc.
- In some cases, such as open source, “adequate” confidentiality means “no confidentiality required”.
- Development resources for backup include, among others, source code, databases, development and operation tools and their configurations.

A.15.4 DEV-04 Separation of Environments

A.15.4.1 Objective

The development environment takes information security in consideration.

A.15.4.2 Requirements

Basic	The <u>CSP</u> shall ensure that <u>production environments</u> are physically or logically separated from <u>development</u> , <u>test</u> or <u>pre-production environments</u> .	DEV-04.1B
	<u>CSC data</u> contained in the <u>production environments</u> shall not be used in <u>development</u> , <u>test</u> or <u>pre-production environments</u> in order not to compromise their confidentiality, unless explicitly requested by CSCs.	DEV-04.2B
Substantial	The <u>CSP</u> shall ensure that <u>production environments</u> are physically or logically separated from <u>development</u> , <u>test</u> or <u>pre-production environments</u> .	DEV-04.1S
	<u>CSC data</u> contained in the <u>production environments</u> shall not be used in <u>development</u> , <u>test</u> or <u>pre-production environments</u> in order not to compromise their confidentiality, unless explicitly requested by CSCs.	DEV-04.2S
	The <u>CSP</u> shall minimize the reuse of cryptographic secrets and private keys and other secrets used in the <u>production environments</u> with other non-production environments.	DEV-04.3S
	Such reuse of cryptographic secrets and private keys and other secrets shall be documented.	DEV-04.4S
High	The <u>CSP</u> shall ensure that <u>production environments</u> are physically or logically separated from <u>development</u> , <u>test</u> or <u>pre-production environments</u> .	DEV-04.1H
	<u>CSC data</u> contained in the <u>production environments</u> shall not be used in <u>development</u> , <u>test</u> or <u>pre-production environments</u> in order not to compromise their confidentiality, unless explicitly requested by CSCs.	DEV-04.2H
	The <u>CSP</u> shall minimize the reuse of the cryptographic secret and private keys and other secrets used in the <u>production environments</u> with other non-production environments.	DEV-04.3H
	Such reuse of cryptographic secrets and private keys and other secrets shall be documented.	DEV-04.4H
	When non-production environments are exposed through public networks, security requirements shall be equivalent to those defined for <u>production environment</u>.	DEV-04.5H

A.15.4.3 Guidance requirements

- There is another requirement (in CCM-03), 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.
- The “equivalence” of security requirements here means that the environments shall satisfy the security requirements associated to the same evaluation level.

A.15.5 DEV-05 Development of Security Features

A.15.5.1 Objective

The development environment takes information security in consideration for the implementation of technical measures or safeguards.

A.15.5.2 Requirements

Basic	The <u>CSP</u> shall <u>define</u> and <u>implement</u> according to ISP-02 specific procedures for the development of security features that implement technical mechanisms or safeguards required by the EUCS, with increased <u>testing requirements</u> .	DEV-05.1B
-------	---	-----------

Substantial	The CSP shall <u>define</u> and <u>implement</u> according to ISP-02 specific procedures for the development of security features that implement technical mechanisms or safeguards required by the EUCS, with increased <u>testing requirements</u> .	DEV-05.1S
	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.	DEV-05.2S
	The <u>tests</u> of the security features shall provide full coverage of the specification, including all specified error conditions.	DEV-05.3S
	The documentation of the tests for security features shall include at least a description of the <u>test</u>, the initial conditions, the expected outcome and instructions for running the <u>test</u>.	DEV-05.4S
High	The CSP shall <u>define</u> and <u>implement</u> according to ISP-02 specific procedures for the development of security features that implement technical mechanisms or safeguards required by the EUCS, with increased <u>testing requirements</u> .	DEV-05.1H
	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.	DEV-05.2H
	The <u>tests</u> of the security features shall provide full coverage of the specification, including all specified error conditions.	DEV-05.3H
	The documentation of the <u>tests</u> for security features shall include at least a description of the <u>test</u> , the initial conditions, the expected outcome and instructions for running the <u>test</u> .	DEV-05.4H
	The documentation of the tests shall include a demonstration of the coverage of the source code, including branch coverage for security-critical code.	DEV-05.5H

A.15.5.3 Guidance requirements

- Full coverage is intended to ensure that all requirements from the specification are tested at least once
- Coverage is demonstrated by providing an analysis of the coverage of the security function specification (and its mapping to implementation) by the tests

A.15.6 DEV-06 Identification of Vulnerabilities of the Cloud Service

A.15.6.1 Objective

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

A.15.6.2 Requirements

Basic	The CSP shall apply appropriate measures to check the <u>cloud service</u> for <u>vulnerabilities</u> that may have been integrated into the <u>cloud service</u> during the development process.	DEV-06.1B
	The <u>procedures</u> for identifying <u>vulnerabilities</u> shall be integrated in the development process	DEV-06.2B
Substantial	The CSP shall apply appropriate measures to check the <u>cloud service</u> for <u>vulnerabilities</u> that may have been integrated into the <u>cloud service</u> during the development process.	DEV-06.1S
	The <u>procedures</u> for identifying <u>vulnerabilities</u> shall be integrated in the development process.	DEV-06.2S
	The <u>procedures</u> for identifying <u>vulnerabilities</u> shall include the following activities, depending on the risk assessment:	DEV-06.3S
	<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 <u>vulnerabilities</u> in software libraries provided by third parties and used in their own cloud service 	
	The CSP shall assess the severity of identified <u>vulnerabilities</u> according to the <u>criteria</u> defined in OPS-17.	DEV-06.4S
	Measures shall be taken to immediately eliminate or mitigate them.	DEV-06.5S

High	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.	DEV-06.1H
	The procedures for identifying vulnerabilities shall be integrated in the development process.	DEV-06.2H
	The procedures for identifying vulnerabilities shall include the following activities, depending on the risk assessment:	DEV-06.3H
	<ul style="list-style-type: none"> • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews and security penetration tests by subject matter experts, as part of the annual programme defined in OPS-19 and prior to making new features available in the production environment; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. 	
	The CSP shall assess the severity of identified vulnerabilities according to the criteria defined in OPS-17.	DEV-06.4H
	Measures shall be taken to immediately eliminate or mitigate them.	DEV-06.5H

A.15.6.3 Guidance requirements

- 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.
- 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.

A.15.7 DEV-07 Outsourcing of the Development

A.15.7.1 Objective

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

A.15.7.2 Requirements

Basic	<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 	DEV-07.1B
Substantial	<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. 	DEV-07.1S
	<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; • Availability of source code to the CSP; • Human resource procedures implemented by the subcontractor; • Required access to the CSP's development, test and pre-production environments; and 	DEV-07.2S

	<ul style="list-style-type: none"> Security procedures related to the management of the subcontractor's supply chain. 	
High	<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. <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; Availability of source code to the CSP; Human resource procedures implemented by the subcontractor; Required access to the CSP's development, test and pre-production environments; and Security procedures related to the management of the subcontractor's supply chain. <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 CSP and makes it possible to achieve a level of security of the external development that matches that of internal development.</p> <p>Personnel of the CSP shall run the tests that are relevant for the deployment decision when a change includes the result of outsourced development.</p>	<p>DEV-07.1H</p> <p>DEV-07.2H</p> <p>DEV-07.3H</p> <p>DEV-07.4H</p>

A.15.7.3 Guidance requirements

- 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.
- 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.
- The requirement on development security is about matching the requirements of the same evaluation level, not about matching point-per-point every feature.

A.15.8 DEV-08 Controlling exchanges with suppliers of functional components

A.15.8.1 Objective

The exchanges with suppliers of functional components are limited and controlled by the CSP.

A.15.8.2 Requirements

Basic	None	
Substantial	<p>When a functional component is used in the provision of the cloud service, and may have access, directly or indirectly, to CSC data, the CSP shall define and implement a policy according to ISP-02 that does not allow such a component to exchange directly with its supplier.</p> <p>When a functional component is used in the provision of the cloud service, and may have access, directly or indirectly, to CSC data, the CSP shall define and implement procedures according to ISP-02 to authorize any content provided by the supplier for its functional components before transferring the content to the functional components.</p> <p>When a functional component is used in the provision of the cloud service, and may have access, directly or indirectly, to CSC data, the CSP shall define and implement procedures according to ISP-02 to authorize any content to be sent from a functional component to its supplier before transferring the content to the supplier.</p>	<p>DEV-08.1H</p> <p>DEV-08.2H</p> <p>DEV-08.3H</p>

	When a <u>procedure</u> to authorize content is automated, then the CSP shall implement this <u>procedure</u> using a solution that keeps traces of the operations proposed by the <u>suppliers</u> , of the verification performed to authorize the content and of the incoming and outgoing transfers effectively performed.	DEV-08.4H
High	When a <u>functional component</u> is used in the provision of the <u>cloud service</u> , and may have access, directly or indirectly, to CSC data, the CSP shall define and implement a policy according to ISP-02 that does not allow such a component to exchange directly with its supplier.	DEV-08.1H
	When a <u>functional component</u> is used in the provision of the <u>cloud service</u> , and may have access, directly or indirectly, to CSC data, the CSP shall define and implement procedures according to ISP-02 to authorize any content provided by the supplier for its <u>functional component</u> before transferring the content to the <u>functional component</u> .	DEV-08.2H
	When a <u>functional component</u> is used in the provision of the <u>cloud service</u> , and may have access, directly or indirectly, to CSC data, the CSP shall define and implement procedures according to ISP-02 to authorize any content to be sent from the <u>functional component</u> to its supplier before transferring the content to the supplier.	DEV-08.3H
	When a <u>procedure</u> to authorize content is automated, then the CSP shall implement this <u>procedure</u> using a solution that keeps traces of the operations proposed by the <u>suppliers</u> , of the verification performed to authorize the content and of the incoming and outgoing transfers effectively performed.	DEV-08.4H

A.15.8.3 Guidance requirements

- The application of the requirement should not interfere with proper asset management, and in particular with the fact that all components shall be maintained up-to-date. The requirements in this category simply give the CSP the right to analyse the content to identify the nature of the exchanges, and if needed of its details (for instance, verifying the authenticity of a software update).
- The DEV-08.2H requirement may for instance apply to incoming flows related to software updates,
- The DEV-08.3H requirement may for instance apply to outgoing flows related to billing, incident logs or supervision metrics.
- The DEV-08.2H and DEV-08.3H requirement may be satisfied by using a dedicated machine in a demilitarized zone (DMZ) to control the exchanges and to perform the required verifications.

A.16 PROCUREMENT MANAGEMENT

ENSURE THE PROTECTION OF INFORMATION THAT SUPPLIERS OF THE CSP CAN ACCESS AND MONITOR THE AGREED SERVICES AND SECURITY REQUIREMENTS

Term	Definition
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]
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	interested party providing services to the CSP that contribute to the provision of the cloud service by the CSP

A.16.1 PM-01 Policies and Procedures for Controlling and Monitoring Third Parties

A.16.1.1 Objective

Policies and procedures are defined to supervise the activities of third parties who contribute to the provision of the cloud service.

A.16.1.2 Requirements

Basic	The CSP shall define and implement policies and procedures according to ISP-02 for controlling and monitoring interested parties whose products or services contribute to the provision of the cloud service.	PM-01.1B
Substantial	<p>The CSP shall define and implement policies and procedures according to ISP-02 for controlling and monitoring interested parties whose products or services contribute to the provision of the cloud service, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Requirements for the assessment of risks resulting from the procurement of products and 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 the personnel of interested parties; • 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 	PM-01.1S

High	<p>The CSP shall define and implement policies and procedures according to ISP-02 for controlling and monitoring interested parties whose products or services contribute to the provision of the cloud service, covering at least the following aspects:</p> <ul style="list-style-type: none"> • Requirements for the assessment of risks resulting from the procurement of third-party products and 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 the personnel of interested parties; • 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. <p>The CSP shall contractually require its subservice providers to provide regular assurance information by independent auditors or CABs on the suitability of the design and operating effectiveness of their service-related internal control system with respect to the EUCS requirements</p> <p>The assurance information shall include the complementary subservice organisation controls that are required, together with the controls of the CSP, to meet the applicable EUCS requirements with reasonable assurance</p> <p>In case the subservice providers are not able to provide an EUCS compliance assurance information 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.</p>	<p>PM-01.1H</p> <p>PM-01.2H</p> <p>PM-01.3H</p> <p>PM-01.4H</p>
------	---	---

A.16.1.3 Guidance requirements

- Note that the term “supplier” covers both third parties that sell products and those who provide services.
- Both the terms “supplier”, “service provider” and “interested party” cover all parties that are outside of the certification scope, even if they are part of the same company. Nevertheless, the activities outsourced to these parties is in the scope of certification. When required, a distinction can be made by qualifying the terms (e.g., “internal supplier” or “external supplier”).
- The requirement PM-01.4H is considered as an acceptable compensating requirement. Here, the right to audit is considered as an alternative to the availability of a proper compliance report.

A.16.2 PM-02 Risk Assessment of Suppliers

A.16.2.1 Objective

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

A.16.2.2 Requirements

Basic	<p>The CSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of interested parties as defined in PM-01, before they start contributing to the provision of the cloud service.</p> <p>The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with subservice providers and suppliers.</p> <p>Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of complementary subservice organisation controls (CSOCs) to be implemented by the subservice provider.</p> <p>The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available to the CSP assurance information supporting the assessment of their suitability for the targeted evaluation level.</p> <p>The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.</p>	<p>PM-02.1B</p> <p>PM-02.2B</p> <p>PM-02.3B</p> <p>PM-02.4B</p> <p>PM-02.5B</p>
-------	--	---

Substantial	<p>The CSP shall perform a risk assessment of its suppliers in accordance with the policies and procedures for the control and monitoring of interested parties, as defined in PM-01, before they start contributing to the provision of the cloud service, including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects:</p> <ul style="list-style-type: none"> • Protection needs regarding the confidentiality, integrity, availability, and authenticity of information processed, stored, or transmitted by the interested party; • Impact of a protection breach on the provision of the cloud service; • The CSP's dependence on the supplier or service provider for the scope, complexity, and uniqueness of the purchased product or service including the consideration of possible alternatives. <p>The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with service providers and suppliers, based on the requirements identified by the CSP for the protection of confidential information and operational details.</p> <p>Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of complementary subservice organisation controls (CSOCs) to be implemented by the subservice provider.</p> <p>The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available to the CSP assurance information supporting the assessment of their suitability and operating effectiveness for the targeted evaluation level.</p> <p>The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.</p>	<p>PM-02.1S</p> <p>PM-02.2S</p> <p>PM-02.3S</p> <p>PM-02.4S</p> <p>PM-02.5S</p>
High	<p>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, including the identification, analysis, evaluation, handling, and documentation of risks concerning the following aspects:</p> <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 supplier or service provider for the scope, complexity, and uniqueness of the purchased product or service, including the consideration of possible alternatives. <p>The CSP shall ensure that non-disclosure or confidentiality agreements are agreed with service providers and suppliers, based on the requirements identified by the CSP for the protection of confidential information and operational details</p> <p>Following the risk assessment of a subservice provider, the CSP shall define for every applicable EUCS requirement a list of complementary subservice organisation controls (CSOCs) to be implemented by the subservice provider.</p> <p>The CSP shall ensure that the subservice provider has implemented the CSOCs, and that the subservice provider has made available to the CSP assurance information supporting the assessment of their suitability and operating effectiveness for the targeted evaluation level.</p> <p>The adequacy of the risk assessment and of the definition of CSOCs shall be reviewed regularly, at least annually.</p> <p>When the CSP relies on products from a supplier to operate the cloud service the CSP shall not allow this supplier to access any CSC data, cloud service derived data or CSC account data, unless they:</p> <ul style="list-style-type: none"> • perform a risk assessment according to RM-01 on the possible exposure of CSC data, cloud service derived data or CSC account data; • inform their CSCs of these possible accesses in contractual documentation; • ensure that all operations requiring access to CSC data, cloud service derived data or CSC account data are performed or supervised by personnel who has been authorized (cf. HR-02.1H). 	<p>PM-02.1H</p> <p>PM-02.2H</p> <p>PM-02.3H</p> <p>PM-02.4H</p> <p>PM-02.5H</p> <p>PM-02.6H</p>

A.16.2.3 Guidance requirements

- 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

A.16.3 PM-03 Directory of Suppliers

A.16.3.1 Objective

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

A.16.3.2 Requirements

Basic	<p>The <u>CSP</u> shall maintain a directory for controlling and monitoring the <u>suppliers</u> who contribute to the delivery of the <u>cloud service</u>.</p> <p>The <u>CSP</u> shall verify the directory for completeness, accuracy and validity at least annually.</p>	<p>PM-03.1B</p> <p>PM-03.2B</p>
Substantial	<p>The <u>CSP</u> shall maintain a directory for controlling and monitoring the <u>suppliers</u> who contribute to the delivery of the <u>cloud service</u>, containing at least the following <u>information</u>:</p> <ul style="list-style-type: none"> • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the <u>supplier</u>; • Responsible contact person at the <u>CSP</u>; • Description of the <u>product or service</u>; • Classification based on the <u>risk assessment</u>; • Beginning of service usage; and • Proof of <u>compliance</u> with contractually agreed <u>requirements</u>. <p>The <u>CSP</u> shall verify the directory for completeness, accuracy and validity at least annually.</p>	<p>PM-03.1S</p> <p>PM-03.2S</p>
High	<p>The <u>CSP</u> shall maintain a directory for controlling and monitoring the <u>suppliers</u> who contribute to the delivery of the <u>cloud service</u>, containing at least the following information:</p> <ul style="list-style-type: none"> • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the <u>supplier</u>; • Responsible contact person at the <u>CSP</u>; • Description of the <u>product or service</u>; • Classification based on the <u>risk assessment</u>; • Beginning of service usage; and • Proof of <u>compliance</u> with contractually agreed <u>requirements</u>. <p>The <u>CSP</u> shall verify the directory for completeness, accuracy and validity at least annually.</p>	<p>PM-03.1S</p> <p>PM-03.2S</p>

A.16.3.3 Guidance requirements

- The centralization objective is intended to ensure that a single directory should be available, but it does not mandate any technology for its implementation

A.16.4 PM-04 Monitoring of Compliance with Requirements

A.16.4.1 Objective

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

A.16.4.2 Requirements

Basic	<p>The <u>CSP</u> shall monitor the compliance of its <u>suppliers</u> with <u>information security</u> requirements and applicable legal and regulatory requirements in accordance with <u>policies and procedures</u> concerning controlling and <u>monitoring of interested parties</u>, as defined in PM-01.</p> <p>The <u>CSP</u> shall monitor the compliance of its subservice providers with the <u>CSOCs</u> applicable to them following the <u>risk assessment</u> (cf. PM-02).</p>	<p>PM-04.1B</p> <p>PM-04.2B</p> <p>PM-04.3B</p>
-------	--	---

	<p>The frequency of the monitoring shall correspond to the classification of the <u>third party</u> based on the <u>risk assessment</u> conducted by the <u>CSP</u> (cf. PM-02).</p> <p>The results of the <u>monitoring</u> shall be considered in the <u>review</u> of the <u>interested party's</u> <u>risk assessment</u>.</p> <p>Identified violations and deviations shall be analysed, evaluated and treated in accordance with the <u>risk management procedure</u> (cf. RM-01).</p> <p>When a change in an <u>interested party</u> contributing to the provision of the cloud service significantly adversely affects its level of security, the <u>CSP</u> shall inform all of its <u>CSCs</u> without undue delay.</p>	<p>PM-04.4B</p> <p>PM-04.5B</p> <p>PM-04.6B</p>
Substantial	<p>The <u>CSP</u> shall monitor the compliance of its <u>suppliers</u> with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and <u>monitoring</u> of <u>interested parties</u>, as defined in PM-01, and including at least a regular review of the following <u>assurance information</u>, as provided by <u>suppliers</u> under contractual agreements:</p> <ul style="list-style-type: none"> • Reports on the quality of the <u>service</u> provided; • Certificates of the <u>management systems'</u> compliance with international standards; • Independent <u>third-party reports</u> on the suitability and <u>operating effectiveness</u> of their <u>service-related internal control systems</u>; and • Records of the <u>interested parties</u> on the handling of <u>vulnerabilities</u>, <u>security incidents</u> and malfunctions. <p>The <u>CSP</u> shall monitor the compliance of its <u>subservice providers</u> with the <u>CSOCs</u> applicable to them following the <u>risk assessment</u> (cf. PM-02).</p> <p>The frequency of the monitoring shall correspond to the classification of the <u>third party</u> based on the <u>risk assessment</u> conducted by the <u>CSP</u> (cf. PM-02).</p> <p>The results of the <u>monitoring</u> shall be considered in the <u>review</u> of the <u>interested party's</u> <u>risk assessment</u>.</p> <p>Identified violations and deviations shall be analysed, evaluated and treated in accordance with the <u>risk management procedure</u> (cf. RM-01).</p> <p>The <u>CSP</u> shall document and implement a procedure to review, at least once a year, <u>non-disclosure or confidentiality requirements</u> regarding <u>suppliers</u> contributing to the provision of the <u>cloud service</u>.</p> <p>When a change in an <u>interested party</u> contributing to the provision of the cloud service significantly adversely affects its level of security, the <u>CSP</u> shall inform all of its <u>CSCs</u> without undue delay.</p>	<p>PM-04.1S</p> <p>PM-04.2S</p> <p>PM-04.3S</p> <p>PM-04.4S</p> <p>PM-04.5S</p> <p>PM-04.7S</p> <p>PM-04.6S</p>
High	<p>The <u>CSP</u> shall monitor the compliance of its <u>suppliers</u> with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and <u>monitoring</u> of <u>interested parties</u>, as defined in PM-01, and including at least a regular review of the following <u>assurance information</u>, as provided by <u>suppliers</u> under contractual agreements:</p> <ul style="list-style-type: none"> • Reports on the quality of the <u>service</u> provided; • Certificates of the <u>management systems'</u> compliance with international standards; • Independent <u>third-party reports</u> on the suitability and <u>operating effectiveness</u> of their <u>service-related internal control systems</u>; and • Records of the <u>interested parties</u> on the handling of <u>vulnerabilities</u>, <u>security incidents</u> and malfunctions. <p>The <u>CSP</u> shall monitor the compliance of its <u>subservice providers</u> with the <u>CSOCs</u> applicable to them following the <u>risk assessment</u> (cf. PM-02).</p> <p>The <u>CSP</u> shall supplement procedures for <u>monitoring compliance</u> with automatic monitoring, by leveraging automatic procedures, when possible, relating to the following aspects:</p> <ul style="list-style-type: none"> • Configuration of <u>system components</u>; • Performance and availability of <u>system components</u>; • Response time to malfunctions and <u>security incidents</u>; and • Recovery time (time until completion of error handling). <p>The <u>CSP</u> shall automatically monitor Identified violations and discrepancies.</p> <p>The identified violations and discrepancies shall be automatically reported to the responsible personnel or <u>system components</u> of the <u>CSP</u> for prompt assessment and action.</p> <p>The frequency of the monitoring shall correspond to the classification of the <u>third party</u> based on the <u>risk assessment</u> conducted by the <u>CSP</u> (cf. PM-02).</p> <p>The results of the <u>monitoring</u> shall be considered in the <u>review</u> of the <u>third party's</u> <u>risk assessment</u>.</p> <p>Identified violations and deviations shall be analysed, evaluated and treated in accordance with the <u>risk management procedure</u> (cf. RM-01).</p>	<p>PM-04.1H</p> <p>PM-04.2H</p> <p>PM-04.8H</p> <p>PM-04.9H</p> <p>PM-04.10H</p> <p>PM-04.3H</p> <p>PM-04.4H</p> <p>PM-04.5H</p>

	The CSP shall document and implement a procedure to review, at least once a year, non-disclosure or confidentiality requirements regarding suppliers contributing to the provision of the cloud service.	PM-04.7H
	When a change in an interested party contributing to the provision of the cloud service significantly adversely affects its level of security, the CSP shall inform all of its CSCs without undue delay.	PM-04.6H

A.16.4.3 Guidance requirements

- The monitoring required at level CS-Substantial includes a documentary review, which should not be too complex, as long as the subservice provider has appropriate assurance information.
- 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

A.16.5 PM-05 Exit Strategy

A.16.5.1 Objective

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

A.16.5.2 Requirements

Basic	The CSP shall define exit strategies for the purchase of products or services where the risk assessment of the suppliers identified a very high dependency.	PM-05.1B
Substantial	<p>The CSP shall define exit strategies for the purchase of products or services where the risk assessment of the suppliers identified a very high dependency, which 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 product or service performance monitoring, which should trigger the withdrawal from the product or service if the results are unacceptable. 	PM-05.1S
High	<p>The CSP shall define exit strategies for the purchase of products or services where the risk assessment of the suppliers identified a very high dependency, which 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 product or service performance monitoring, which should trigger the withdrawal from the product or service if the results are unacceptable. <p>When the CSP relies for the provision of the cloud service on products or services from a supplier for which the CSP has identified a very high dependency (cf. PM-05.1H), then in case of contract termination, the CSP shall be guaranteed contractually by its supplier the ability to maintain the operation of its cloud service under normal conditions for a specified period of time, and the CSP shall indicate this period of time in contractual agreements with CSCs.</p>	<p>PM-05.1H</p> <p>PM-05.2H</p>

A.16.5.3 Guidance requirements

- Exit strategies are related to business continuity, and are expected to be considered as part of the testing activities for business continuity

POLITICO

A.17 INCIDENT MANAGEMENT

ENSURE A CONSISTENT AND COMPREHENSIVE APPROACH TO THE CAPTURE, ASSESSMENT, COMMUNICATION AND ESCALATION OF SECURITY INCIDENTS

Term	Definition
information security event	occurrence indicating a possible breach of information security or failure of controls [SOURCE: From ISO/IEC 27035-1:2016, 3.3]
information security incident	one or multiple related and identified information security events that can harm an organization's assets or compromise its operations [SOURCE: From ISO/IEC 27035-1:2016, 3.4]
incident handling	actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents [SOURCE: From ISO/IEC 27035-1:2016, 3.6]
incident response	actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it [SOURCE: From ISO/IEC 27035-1:2016, 3.7]
point of contact	defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities [SOURCE: From ISO/IEC 27035-1:2016, 3.8]

A.17.1 IM-01 Policy for Security Incident Management

A.17.1.1 Objective

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

A.17.1.2 Requirements

Basic	<p>The CSP shall define 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, including</p> <ul style="list-style-type: none"> Guidelines for the classification, prioritization, and escalation of security incidents; Description of interfaces for incident management and business continuity management. <p>The CSP shall establish a point of contact, which contributes to the coordinated resolution of security incidents.</p>	<p>IM-01.1B</p> <p>IM-01.2B</p>
Substantial	<p>The CSP shall define 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, including</p> <ul style="list-style-type: none"> Guidelines for the classification, prioritization, and escalation of security incidents; Description of interfaces for incident management and business continuity management; Procedures as to how the data of a potentially impacted system can be collected in a conclusive manner in the event of a security incident. <p>The CSP shall establish a Computer Security Incident Response Team (CSIRT), which contributes to the coordinated resolution of security incidents.</p>	<p>IM-01.1S</p> <p>IM-01.2S</p>

	The CSP shall inform the CSCs affected by security incidents in a timely and appropriate manner.	IM-01.3S
High	<p>The CSP shall define 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, including</p> <ul style="list-style-type: none"> • Guidelines for the classification, prioritization, and escalation of security incidents; • Description of interfaces for incident management and business continuity management; • Procedures as to how the data of a potentially impacted system can be collected in a conclusive manner in the event of a security incident; • Analysis plans for typical security incidents; • An evaluation methodology so that the collected information does not lose its evidential value in any subsequent legal assessment; • Provisions for the regular testing of the incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential deficiencies. <p>The CSP shall establish a Computer Security Incident Response Team (CSIRT), which contributes to the coordinated resolution of security incidents.</p> <p>The CSP shall inform the CSCs affected by security incidents in a timely and appropriate manner.</p>	<p>IM-01.1H</p> <p>IM-01.2H</p> <p>IM-01.3H</p>

A.17.1.3 *Guidance requirements*

- At level Basic, the point of contact is intended as an equivalent to the CERT, as a simplified organization that supervises the response to incidents
- Refer to the EU blueprint for cooperative response to large-scale cross-border cybersecurity incidents

A.17.2 IM-02 Handling of Security Incidents

A.17.2.1 Objective

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

A.17.2.2 Requirements

Basic	The CSP shall classify and prioritize security events that could constitute a security incident, and perform root-cause analyses for these events, using their subject matter experts and external security providers where appropriate.	IM-02.1B
Substantial	The CSP shall classify and prioritize security events that could constitute a security incident, and perform root-cause analyses for these events, using their subject matter experts and external security providers where appropriate.	IM-02.1S
	The CSP shall maintain a catalogue that clearly identifies the security incidents that affect CSC data, and use that catalogue to classify security incidents.	IM.02.2S
	The incident classification mechanism shall include provisions to correlate security events.	IM-02.3S
	These correlated security events shall themselves be assessed and classified according to their criticality.	IM-02.4S
High	The CSP shall classify and prioritize security events that could constitute a security incident, and perform root-cause analyses for these events, using their subject matter experts and external security providers where appropriate.	IM-02.1H
	The CSP shall maintain a catalogue that clearly identifies the security incidents that affect CSC data, and use that catalogue to classify security incidents.	IM.02.2H
	The incident classification mechanism shall include provisions to correlate security events.	IM-02.3H
	These correlated security events shall themselves be assessed and classified according to their criticality.	IM-02.4H
	The CSP shall simulate the identification, analysis, and defence of security incidents and attacks at least once a year through appropriate tests and exercises.	IM.02.5H IM-02.5H

The CSP shall automatically monitor the processing of security incidents to verify the application of incident management policies and procedures

A.17.2.3 Guidance requirements

- Correlation of events should be performed within limits to be defined by the CSP, with the objective of associating related events that may indicate an incident
- Simulations could include activities like Red Team training.
- Typical monitoring could occur through analysis a ticket management or other business process management system

A.17.3 IM-03 Documentation and Reporting of Security Incidents

A.17.3.1 Objective

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

A.17.3.2 Requirements

Basic	The CSP shall document the implemented measures after a security incident has been handled.	IM-03.1B
	In accordance with contractual agreements between CSP and CSC, information shall be made available to the affected CSCs for final acknowledgment or, if applicable, as confirmation.	IM-03.2B
	The CSP shall make information on security incidents or confirmed security breaches available to all affected CSCs.	IM-03.3B
Substantial	The CSP shall document the implemented measures after a security incident has been handled.	IM-03.1S
	In accordance with the contractual agreements between CSP and CSC, the information shall be made available to the affected CSCs for final acknowledgment or, if applicable, as confirmation.	IM-03.2S
	The CSP shall make information on security incidents or confirmed security breaches available to all affected CSCs.	IM-03.3S
High	The CSP shall document the implemented measures after a security incident has been handled.	IM-03.1H
	In accordance with the contractual agreements between CSP and CSC, the information shall be made available to the affected CSCs for final acknowledgment or, if applicable, as confirmation.	IM-03.2H
	The CSP shall make information on security incidents or confirmed security breaches available to all affected CSCs.	IM-03.3H

A.17.3.3 Guidance requirements

- The approval by customers is intended to ensure that they have enough time to adapt to the change, with a maximum time fixed in contractual clauses, but there is no option for delaying the implementation of the solution past that agreed time.

A.17.4 IM-04 User's Duty to Report Security Incidents

A.17.4.1 Objective

Users are aware of their obligations to report security incidents related to the cloud service.

A.17.4.2 Requirements

Basic	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.	IM-04.1B
	The CSP shall not take any negative action against those who report in good faith events that do not subsequently turn out to be security incidents.	IM-04.2B
	The CSP shall make that policy known as part of its communication to employees and external business partners.	IM-04.3B
	The CSP shall define, publish and implement a single point of contact to receive reports of security events and vulnerabilities.	IM-04.4B
Substantial	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.	IM-04.1S
	The CSP shall not take any negative action against those who report in good faith events that do not subsequently turn out to be security incidents.	IM-04.2S
	The CSP shall make that policy known as part of its communication to employees and external business partners.	IM-04.3S
	The CSP shall define, publish and implement a single point of contact to receive reports of security events and vulnerabilities.	IM-04.4S
High	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.	IM-04.1H
	The CSP shall not take any negative action against those who report in good faith events that do not subsequently turn out to be security incidents.	IM-04.2H
	The CSP shall make that policy known as part of its communication to employees and external business partners.	IM-04.3H
	The CSP shall define, publish and implement a single point of contact to receive reports of security events and vulnerabilities.	IM-04.4H

A.17.4.3 Guidance requirements

- Note that the publication of the single point of contact is an EUCSA requirement

A.17.5 IM-05 Involvement of Cloud Customers in the Event of Incidents

A.17.5.1 Objective

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

A.17.5.2 Requirements

Basic	The CSP shall periodically inform its CSCs on the status of the security incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual agreements.	IM-05.1B
	As soon as a security incident has been closed, the CSP shall inform the affected CSCs about the actions taken, according to the contractual agreements.	IM-05.2B
Substantial	The CSP shall periodically inform its CSCs on the status of the security incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual agreements.	IM-05.1S
	As soon as a security incident has been closed, the CSP shall inform the affected CSCs about the actions taken, according to the contractual agreements.	IM-05.2S
High	The CSP shall periodically inform its CSCs on the status of the security incidents affecting the CSC, or, where appropriate and necessary, involve them in the resolution, according to the contractual agreements.	IM-05.1H

	As soon as a security incident has been closed, the CSP shall inform the affected CSCs about the actions taken, according to the contractual agreements.	IM-05.2H
	The CSP shall define procedures to be described in CSC contractual agreements, defining and describing the involvement of the CSC in the acknowledgement of a solution to an incident's root cause over a specified period.	IM-05.3H

A.17.5.3 Guidance requirements

-

A.17.6 IM-06 Evaluation and Learning Process

A.17.6.1 Objective

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

A.17.6.2 Requirements

Basic	The CSP shall perform an analysis of security incidents to identify recurrent or significant security events or incidents and to identify the need for further protection, if needed with the support of external bodies.	IM-06.1B
	If the CSP determines the need for external assistance, it shall select a competent and trustworthy incident response service provider or one that is recommended by its National Cybersecurity Certification Authority (NCCA)	IM-06.2B
Substantial	The CSP shall perform an analysis of security incidents to identify recurrent or significant security events or incidents and to identify the need for further protection, if needed with the support of external bodies.	IM-06.1S
	If the CSP determines the need for external assistance, it shall select a competent and trustworthy incident response service provider or one that is recommended by its National Cybersecurity Certification Authority (NCCA).	IM-06.2S
	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 security incidents affected.	IM-06.3S
	The CSP shall use that information to enrich the classification catalogue of incidents (cf. IM-02).	IM-06.4S
	The intelligence gained from the incident management and gathered in the knowledge repository shall be used to identify recurring security events or incidents, or potential significant security incidents, to determine the need for advanced safeguards, and implement them.	IM-06.5S
High	The CSP shall perform an analysis of security incidents to identify recurrent or significant security events or incidents and to identify the need for further protection, if needed with the support of external bodies.	IM-06.1H
	If the CSP determines the need for external assistance, it shall select a competent and trustworthy incident response service provider or one that is recommended by its National Cybersecurity Certification Authority (NCCA).	IM-06.2H
	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 security incidents affected.	IM-06.3H
	The CSP shall use that information to enrich the classification catalogue of incidents (cf. IM-02).	IM-06.4H
	The intelligence gained from the incident management and gathered in the knowledge repository shall be used to identify recurring security events or incidents, or potential significant security incidents, to determine the need for advanced safeguards, and implement them.	IM-06.5H

A.17.6.3 Guidance requirements

- Explain the idea of knowledge repository and how it can take a simple form

A.17.7 IM-07 Incident Evidence Preservation

A.17.7.1 Objective

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

A.17.7.2 Requirements

Basic	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents related to the cloud service.	IM-07.1B
	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.	IM-07.2B
Substantial	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents related to the cloud service, in a way that could be used as evidence in court.	IM-07.1S
	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.	IM-07.2S
	When the CSP requires additional expertise in order to preserve the evidence and secure the chain of custody on a security incident, the CSP shall contract a qualified incident response service provider only.	IM-07.3S
High	The CSP shall document and implement a procedure to archive all documents and evidence that provide details on security incidents related to the cloud service, in a way that could be used as evidence in court.	IM-07.1H
	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.	IM-07.2H
	The CSP shall establish, or contract for the services of, an integrated team of forensic/incident responder personnel specifically trained on evidence preservation and chain of custody management.	IM-07.4H
	When the CSP requires additional expertise in order to preserve the evidence and secure the chain of custody on a security incident, the CSP shall contract a qualified incident response service provider only.	IM-07.3H

A.17.7.3 Guidance requirements

- Explain the idea of knowledge repository and how it can take a simple form

A.18 BUSINESS CONTINUITY

PLAN, IMPLEMENT, MAINTAIN AND TEST PROCEDURES AND MEASURES FOR BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT

Term	Definition
business continuity	capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption [SOURCE: From ISO 22301:2019, 3.3]
business continuity plan	documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives [SOURCE: From ISO 22301:2019, 3.4]
business impact analysis	process of analysing the impact over time of a disruption on the organization Note 1 to entry: The outcome is a statement and justification of business continuity requirements. [SOURCE: From ISO 22301:2019, 3.5]
disruption	incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives [SOURCE: From ISO 22301:2019, 3.10]
impact	outcome of a disruption affecting objectives [SOURCE: From ISO 22301:2019, 3.10]

A.18.1 BC-01 Business Continuity Policies and Top Management Responsibility

A.18.1.1 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.

A.18.1.2 Requirements

Basic	The CSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure <u>business continuity</u> and contingency management.	BC-01.1B
Substantial	The CSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure business continuity and contingency management.	BC-01.1S
	The CSP shall name at least one member of top management as the process owner of <u>business continuity</u> and emergency management for the cloud service.	BC-01.2S
	The process owner shall be responsible for establishing the process within the company following the strategy as well as ensuring compliance with the guidelines.	BC-01.3S
	The process owner shall be responsible for ensuring that sufficient resources are made available for an effective process	BC-01.4S
High	The CSP shall define policies and procedures according to ISP-02 establishing the strategy and guidelines to ensure business continuity and contingency management.	BC-01.1H
	The CSP shall name (at least one member of) top management as the process owner of <u>business continuity</u> and emergency management.	BC-01.2H

	The process owner shall be responsible for establishing the <u>process</u> within the company following the strategy as well as ensuring <u>compliance</u> with the guidelines.	BC-01.3H
	The process owner shall be responsible for ensuring that sufficient resources are made available for an effective <u>process</u> .	BC-01.4H

A.18.1.3 *Guidance requirements*

- BC should be endorsed by top management at all levels, but at level Substantial, the requirements are explicit and more detailed.

A.18.2 BC-02 Business Impact Analysis Procedures

A.18.2.1 Objective

The business continuity framework is based on a business impact analysis.

A.18.2.2 Requirements

Basic	The policies and procedures for business continuity and contingency management shall include the need to perform a <u>business impact analysis</u> to determine the impact of any malfunction to the <u>cloud service</u> or enterprise.	BC-02.1B
Substantial	<p>The policies and procedures for business continuity and contingency management shall include the need to perform a <u>business impact analysis</u> to determine the impact of any malfunction to the cloud service or enterprise, considering at least the following aspects:</p> <ul style="list-style-type: none"> • Possible scenarios based on a <u>risk assessment</u>; • Identification of critical <u>products</u> and <u>services</u>; • Identification of dependencies, including <u>processes</u> (including resources required), applications, business partners and other interested 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 <u>products</u> and <u>services</u> 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. <p>The <u>business impact analysis</u> 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.</p>	BC-02.1S BC-02.2S
High	<p>The policies and <u>procedures</u> for business continuity and contingency management shall include the need to perform a <u>business impact analysis</u> to determine the impact of any malfunction to the cloud service or enterprise, considering at least the following aspects:</p> <ul style="list-style-type: none"> • Possible scenarios based on a <u>risk assessment</u>; • Identification of critical <u>products</u> and <u>services</u>; • Identification of dependencies, including <u>processes</u> (including resources required), applications, business partners and other interested parties; • Identification of <u>threats</u> 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 <u>products</u> and <u>services</u> 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. <p>The <u>business impact analysis</u> 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.</p>	BC-02.1H BC-02.2H

A.18.2.3 Guidance requirements

-

A.18.3 BC-03 Business Continuity and Contingency Planning

A.18.3.1 Objective

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

A.18.3.2 Requirements

Basic	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.	BC-03.1B
Substantial	<p>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, based on industry accepted standards, and covering at least the following aspects:</p> <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 and approval; • Defined communication channels, roles and responsibilities including notification of the customers; • 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); • List of standards being used; • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management. <p>The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.</p>	BC-03.1S BC-03.2S
High	<p>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, based on industry accepted standards, and covering at least the following aspects:</p> <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 and approval; • Defined communication channels, roles and responsibilities including notification of the customers; • 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); • List of standards being used; • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management. <p>The business continuity plan shall be reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.</p>	BC-03.1H BC-03.2H

A.18.3.3 Guidance requirements

- The plan also needs to be improved after each testing (cf. BC-04.2), as part of the continuous improvement process

A.18.4 BC-04 Business Continuity Tests and Exercises

A.18.4.1 Objective

The business continuity framework is tested on a regular basis.

A.18.4.2 Requirements

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

A.18.4.3 Guidance requirements

- The results of the tests should be disclosed to CSCs, without providing full details, which would be confidential.

A.19 COMPLIANCE

AVOID NON-COMPLIANCE WITH LEGAL, REGULATORY, SELF-IMPOSED OR CONTRACTUAL INFORMATION SECURITY AND COMPLIANCE REQUIREMENTS

Term	Definition
internal audit	audit where the audit team belongs to the auditee [SOURCE: From ISO14050:2020, 3.4.40]
audit programme	arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose [SOURCE: ISO 19011:2018, 3. 4]

A.19.1 CO-01 Identification of Applicable Compliance Requirements

A.19.1.1 Objective

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

A.19.1.2 Requirements

Basic	The CSP shall document the legal, regulatory, self-imposed and contractual requirements applicable to the information security of the cloud service.	CO-01.1B
Substantial	The CSP shall document the legal, regulatory, self-imposed and contractual requirements applicable to the information security of the cloud service.	CO-01.1S
	The CSP shall document and implement procedures for complying to these contractual requirements.	CO-01.2S
High	The CSP shall document the legal, regulatory, self-imposed and contractual requirements applicable to the information security of the cloud service.	CO-01.1H
	The CSP shall document and implement procedures for complying to these contractual requirements.	CO-01.2H
	The CSP shall provide an overview or summary of these procedures when requested by a CSC.	CO-01.3H
	The CSP shall document and implement a proactive approach for receiving up-to-date legal, regulatory and contractual requirements that affect the cloud service.	CO-01.4H

A.19.1.3 Guidance requirements

- Typically, such requirements may include:
 - Requirements for the protection of personal data (e.g. EU General Data Protection Regulation);
 - Compliance requirements based on contractual obligations with cloud customers (e.g. ISO/IEC 27001, SOC 2, PCI-DSS);
 - Generally accepted accounting principles (e.g. in accordance with HGB or IFRS);
 - National laws
- At level Basic, the compliance requirements remain informal, so procedures are not required.
- The procedures to be shared with customers are high-level procedures, without any confidential information

A.19.2 CO-02 Policy for Planning and Conducting Audits

A.19.2.1 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.

A.19.2.2 Requirements

Basic	The CSP shall define and implement policies and procedures, made in accordance with ISP-02 for planning and conducting audits that protect the operation of the cloud service from interference by audits	CO-02.1B
Substantial	<p>The CSP shall define and implement policies and procedures, made in accordance with ISP-02 for planning and conducting audits that protect the operation of the cloud service from interference by audits, 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 audit 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. <p>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</p>	CO-02.1S CO-02.2S
High	<p>The CSP shall define and implement policies and procedures, made in accordance with ISP-02 for planning and conducting audits that protect the operation of the cloud service from interference by audits, 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 audit 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. <p>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.</p> <p>The CSP shall grant its CSCs contractually guaranteed information and define their audit rights.</p>	CO-02.1H CO-02.2H CO-02.3H

A.19.2.3 Guidance requirements

- The requirement about 3-year planning is about an audit programme, i.e., a high-level planning of the audits to take place in the coming three years, not about building a detailed audit plan for these audits.
- The requirement on audit rights does not mandate that the customers be granted any audit rights, unless required by EU or National law, only that the audit rights that are (or not) granted to them should be contractually defined

A.19.3 CO-03 Internal Audits of the Internal Control System

A.19.3.1 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.

A.19.3.2 Requirements

Basic	The CSP shall perform at regular intervals and at least annually internal audits by subject matter experts that ensure the objectivity and the impartiality of the audit process, to check the compliance of their internal security control system to the	CO-03.1B
-------	--	----------

	<p>requirements defined in CO-01, and to the requirements of the EUCS scheme at the targeted evaluation level.</p> <p>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.</p>	CO-03.2B
Substantial	<p>The CSP shall perform at regular intervals and at least annually internal audits by subject matter experts that ensure the objectivity and the impartiality of the audit process, to check the compliance of their internal security control system to the requirements defined in CO-01, and to the requirements of the EUCS scheme at the targeted evaluation level.</p> <p>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).</p> <p>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.</p> <p>The CSP shall inform CSCs who operate a certified cloud service of nonconformities relatively to EUCS requirements.</p>	<p>CO-03.1S</p> <p>CO-03.3S</p> <p>CO-03.2S</p> <p>CO-03.4S</p>
High	<p>The CSP shall perform at regular intervals and at least annually internal audits by subject matter experts that ensure the objectivity and the impartiality of the audit process, to check the compliance of their internal security control system to the requirements defined in CO-01, and to the requirements of the EUCS scheme at the targeted evaluation level.</p> <p>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).</p> <p>Internal audits shall be supplemented by procedures to automatically monitor compliance with applicable requirements of policies and procedures.</p> <p>The CSP shall implement monitoring to identify vulnerabilities and deviations.</p> <p>The vulnerabilities and deviations shall be reported to the appropriate CSP's subject matter experts for immediate assessment and action.</p> <p>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.</p> <p>The CSP shall inform CSCs who operate an certified cloud service of nonconformities relatively to EUCS requirements.</p>	<p>CO-03.1H</p> <p>CO-03.3H</p> <p>CO-03.5H</p> <p>CO-03.6H</p> <p>CO-03.7H</p> <p>CO-03.2H</p> <p>CO-03.4H</p>

A.19.3.3 Guidance requirements

- The EUCS-related requirements may remain as part of EUCS, even if a Technical Specification is established

A.19.4 CO-04 Information on Internal Control System Assessment

A.19.4.1 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

A.19.4.2 Requirements

Basic	The CSP shall regular inform its top management about the information security performance within the scope of the internal control system for the cloud service.	CO-04.1B
Substantial	<p>The CSP shall regular inform its top management about the information security performance within the scope of the internal control system for the cloud service.</p> <p>This information shall be included in the management review of the internal control system that is performed at least once a year.</p>	<p>CO-04.1S</p> <p>CO-04.2S</p>
High	<p>The CSP shall regular inform its top management about the information security performance within the scope of the internal control system for the cloud service.</p> <p>This information shall be included in the management review of the internal control system that is performed at least once a year.</p>	<p>CO-04.1H</p> <p>CO-04.2H</p>

A.19.4.3 *Guidance requirements*

- The information shared should include at least some information about the result of the audits, including findings, and the remediation actions.

POLITICO

A.20 USER DOCUMENTATION

PROVIDES UP-TO-DATE INFORMATION ON THE SECURE CONFIGURATION AND KNOWN VULNERABILITIES OF THE CLOUD SERVICE FOR CLOUD CUSTOMERS

Term	Definition

A.20.1 DOC-01 Guidelines and Recommendations for Cloud Customers

A.20.1.1 Objective

Provide [information](#) to assist the [CSC](#) in the secure configuration, installation and use of the [cloud service](#).

A.20.1.2 Requirements

Basic	<p>The CSP shall make publicly available guidelines and recommendations to assist the cloud service users with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided.</p> <p>The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use.</p>	<p>DOC-01.1B</p> <p>DOC-01.2B</p>
Substantial	<p>The CSP shall make publicly available guidelines and recommendations to assist the cloud service users with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided, covering at least the following aspects, where applicable to the cloud service:</p> <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 policies including combinations that result in an elevated risk; • Services and functions for administration of the cloud service by privileged users; • Complementary User Entity Controls (CUECs); • Encryption mechanisms and services; • Data leakage prevention; • Secure development of defensive mechanisms, e.g., payload filtering, traffic shaping, load balancing, load shedding, DDoS defences; and • Use and configuration of wide-area distributed architecture mechanisms, e.g., replication for fault tolerance, multiple cloud regions to avoid localised outages and disasters, geo-dispersion of service endpoints to reduce user-facing latency. <p>The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use.</p> <p>The CSP shall describe in the user documentation all risks shared with the CSC.</p>	<p>DOC-01.1S</p> <p>DOC-01.2S</p> <p>DOC-01.3S</p>
High	<p>The CSP shall make publicly available guidelines and recommendations to assist the cloud service users with the secure configuration, installation, deployment, operation and maintenance of the cloud service provided, covering at least the following aspects, where applicable to the cloud service:</p> <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 policies including combinations that result in an elevated risk; 	DOC-01.1H

	<ul style="list-style-type: none"> Services and functions for administration of the cloud service by privileged users, and Complementary User Entity Controls (CUECs); Encryption mechanisms and services; Data leakage prevention; Secure development of defensive mechanisms e.g., payload filtering, traffic shaping, load balancing, load shedding, DDoS defences; and Use and configuration of wide-area distributed architecture mechanisms, e.g., replication for fault tolerance, multiple cloud regions to avoid localised outages and disasters, geo-dispersion of service endpoints to reduce user-facing latency. 	DOC-01.2H DOC-01.3H DOC-01.4H
	<p>The CSP shall maintain guidelines and recommendations applicable to the cloud service in the version intended for productive use.</p> <p>The CSP shall describe in the user documentation all risks shared with the CSC.</p> <p>The CSP shall regularly analyse how the CSCs apply the security recommendations and CUECs and take measures to encourage compliance based on the defined shared responsibility model.</p>	

A.20.1.3 Guidance requirements

- The basis of the requirement on “public availability” of the documentation comes from the EUCSA’s Article 55 of the EUCSA. Here, the documentation may be available without conditions, but only on request
- The documentation of risks is a consequence of the acceptance of risk by risk owners in the risk management procedures (cf. RM-03). Add reference to CCCs
- When a CSP transfers a risk to its customers, this must be reflected in the documentation, although not necessarily explicitly, but the expectation from customers and the associated risk must be described.

A.20.2 DOC-02 Locations of Data Processing and Storage

A.20.2.1 Objective

The CSP provides transparent information about the location of the data and of its processing.

A.20.2.2 Requirements

Basic	<p>The CSP shall provide comprehensible and transparent information on:</p> <ul style="list-style-type: none"> Its jurisdiction; and System component locations, including its subservice providers, where CSC data is processed, stored and backed up. <p>The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service’s jurisdiction and locations from a legal and regulatory perspective.</p>	DOC-02.1B DOC-02.2B
Substantial	<p>The CSP shall provide comprehensible and transparent information on:</p> <ul style="list-style-type: none"> Its jurisdiction; and System component locations, including its subservice providers, where CSC data, meta-data, cloud service derived data and CSC account data is processed, stored and backed up; The locations from which administration and supervision may be carried out on the cloud service. <p>The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service’s jurisdiction and locations from a legal and regulatory perspective.</p>	DOC-02.1S DOC-02.2S
High	<p>The CSP shall provide comprehensible and transparent information on:</p> <ul style="list-style-type: none"> Its jurisdiction; and System component locations, including its subservice providers, where CSC data, meta-data, cloud service derived data and CSC account data is processed, stored and backed up; System component locations, including for its subservice providers, where any CSP data is processed, stored, and backed up; The locations from which administration and supervision may be carried out on the cloud service. 	DOC-02.1H

	<ul style="list-style-type: none"> The locations from which the CSP conducts support operations for CSCs including the list of operations that can be carried by support teams in each location. <p>The CSP shall provide sufficient information for subject matter experts of the CSC to determine and to assess the suitability of the cloud service's jurisdiction and locations from a legal and regulatory perspective.</p>	DOC-02.2H
--	---	-----------

A.20.2.3 Guidance requirements

- The scheme templates provide a detailed description of the kind of information expected.
- The jurisdiction information only includes simple information about where a judicial procedure may be initiated.
- All locations where the cloud service may operate have to be listed, including backup or secondary locations.

A.20.3 DOC-03 Justification of the Targeted Evaluation Level

A.20.3.1 Objective

A rationale is provided for the evaluation level target for the cloud service.

A.20.3.2 Requirements

Basic	The CSP shall provide a justification for the evaluation level targeted for certification, based on the <u>risks</u> associated to the cloud service's targeted customers and use cases.	DOC-03.1B
	If the CSP claims compliance to extension profiles for its <u>cloud service</u> , the justification shall cover these <u>extension profiles</u>	DOC-03.2B
	A summary of the justification shall be <u>made publicly available</u> as part of the <u>certification package</u> .	DOC-03.3B
	The summary shall allow <u>CSCs</u> to perform a high-level analysis about their own use cases.	DOC-03.4B
	The <u>CSP</u> shall make available to their <u>CSCs</u> a mapping of contractual clauses to the cloud service's <u>certification requirements</u> that require such clauses, together with an informal summary of these clauses.	DOC-03.5B
Substantial	The <u>CSP</u> shall provide a justification, <u>based on a risk assessment according to RM-01</u> , for the evaluation level targeted for certification, based on the <u>risks</u> associated to the <u>cloud service's</u> targeted customers and use cases.	DOC-03.1S
	If the <u>CSP</u> claims <u>compliance to extension profiles</u> for its <u>cloud service</u> , the justification shall cover these <u>extension profiles</u> .	DOC-03.2S
	A summary of the justification shall be <u>made publicly available</u> as part of the <u>certification package</u> .	DOC-03.3S
	The summary shall allow <u>CSCs</u> to perform a high-level analysis about their own use cases.	DOC-03.4S
	The <u>CSP</u> shall make available to their <u>CSCs</u> a mapping of contractual clauses to the <u>cloud service's certification requirements</u> that require such clauses, together with an informal summary of these clauses.	DOC-03.5S
High	The <u>CSP</u> shall provide a justification, <u>based on a risk assessment according to RM-01</u> , for the evaluation level targeted for certification, based on the <u>risks</u> associated to the <u>cloud service's</u> targeted customers and use cases.	DOC-03.1S
	If the <u>CSP</u> claims <u>compliance to extension profiles</u> for its <u>cloud service</u> , the justification shall cover these <u>extension profiles</u> .	DOC-03.2S
	A summary of the justification shall be <u>made publicly available</u> as part of the <u>certification package</u> .	DOC-03.3S
	The summary shall allow <u>CSCs</u> to perform a high-level analysis about their own use cases.	DOC-03.4H
	The <u>CSP</u> shall make available to their <u>CSCs</u> a mapping of contractual clauses to the <u>cloud service's certification requirements</u> that require such clauses, together with an informal summary of these clauses.	DOC-03.5H

A.20.3.3 Guidance requirements

- The scheme templates provide a detailed description of the kind of information expected.
-

A.20.4 DOC-04 Guidelines and Recommendations for Composition

A.20.4.1 Objective

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

A.20.4.2 Requirements

Basic	If a CSP wants to allow CSCs to certify with EUCS their own cloud services based on the CSP's cloud service using composition, the CSP shall develop specific documentation and make it available to CSCs upon request, based on the complementary user entity controls (CUECs) that they have defined.	DOC-04.1B
	The CSP shall include in the description provided for each CUEC a list of actionable requirements for the CSC.	DOC-04.2B
	The CSP shall associate each CUEC to at least one EUCS requirement.	DOC-04.3B
Substantial	If a CSP wants to allow CSCs to certify with EUCS their own cloud services based on the CSP's cloud service using composition, the CSP shall develop specific documentation and make it available to CSCs upon request, based on the complementary user entity controls (CUECs) that they have defined.	DOC-04.1S
	The CSP shall include in the description provided for each CUEC a list of actionable requirements for the CSC.	DOC-04.2S
	The CSP shall associate each CUEC to at least one EUCS requirement.	DOC-04.3S
	The CSP shall label each requirement associated to a CUEC with the lowest EUCS evaluation level for which the CUEC is required.	DOC-04.4S
High	If a CSP wants to allow CSCs to certify with EUCS their own cloud services based on the CSP's cloud service using composition, the CSP shall develop specific documentation and make it available to CSCs upon request, based on the complementary user entity controls (CUECs) that they have defined.	DOC-04.1S
	The CSP shall include in the description provided for each CUEC a list of actionable requirements for the CSC.	DOC-04.2S
	The CSP shall associate each CUEC to at least one EUCS requirement.	DOC-04.3S
	The CSP shall label each requirement associated to a CUEC with the lowest EUCS evaluation level for which the CUEC is required.	DOC-04.4H

A.20.4.3 Guidance requirements

- A CSC targeting a specific evaluation level should be able to get the full list of CUEC's that they need to fulfil from that documentation.

A.20.5 DOC-05 Contribution to the Fulfilment of Requirements for Composition

A.20.5.1 Objective

Provide the information needed by customers that want to use the CSP as subservice provider for their own certified cloud service

A.20.5.2 Requirements

Basic	If a CSP wants to allow CSCs to certify with EUCS their own cloud service based on the CSP's cloud service using composition, it shall document for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of this requirement by the cloud service developed by the CSC using the CSP as subservice provider.	DOC-05.1B
	The CSP shall make this documentation available to CSCs upon request.	DOC-05.2B
Substantial	If a CSP wants to allow CSCs to certify with EUCS their own cloud service based on the CSP's cloud service using composition, it shall document for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of this requirement by the cloud service developed by the CSC using the CSP as subservice provider.	DOC-05.1S
	The CSP shall make this documentation available to CSCs upon request.	DOC-05.2S
	The CSP shall justify the contributions in an accompanying document.	DOC-05.3S
High	If a CSP wants to allow CSCs to certify with EUCS their own cloud service based on the CSP's cloud service using composition, it shall document for each EUCS requirement how its cloud service will contribute (if any) to the fulfilment of this requirement by the cloud service developed by the CSC using the CSP as subservice provider.	DOC-05.1H
	The CSP shall make this documentation available to CSCs upon request.	DOC-05.2H
	The CSP shall justify the contributions in an accompanying document.	DOC-05.3H

A.20.5.3 Guidance requirements

- A CSC targeting a specific evaluation level should be able to use this documentation to justify that the base service is fulfilling the requirements.

A.21 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

Term	Definition

A.21.1 INQ-01 Legal Assessment of Investigative Inquiries

A.21.1.1 Objective

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

A.21.1.2 Requirements

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

A.21.1.3 Guidance requirements

- Subject matter experts are legal experts in that case.
- The requirements in INQ are not intended in any way to delay or hinder investigations, but only to provide guarantees to CSCs that processes are defined and applied for the handling of such requests
- The objective is here to ensure that CSPs perform due diligence when receiving requests from governments and are appropriately transparent about these requests

A.21.2 INQ-02 Informing Cloud Customers about Investigation Requests

A.21.2.1 Objective

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

A.21.2.2 Requirements

Basic	The CSP shall inform the affected CSC(s) about investigation requests without undue delay, unless the applicable legal basis on which the government action is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	INQ-02.1B
Substantial	The CSP shall inform the affected CSC(s) about investigation requests without undue delay, unless the applicable legal basis on which the government action is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	INQ-02.1S
High	The CSP shall inform the affected CSC(s) about investigation requests without undue delay, unless the applicable legal basis on which the government action is based prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	INQ-02.1H

A.21.2.3 Guidance requirements

-

A.21.3 INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests

A.21.3.1 Objective

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

A.21.3.2 Requirements

Basic	The CSP shall only provide access to or disclose CSC 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.	INQ-03.1B
	The CSP shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate.	INQ-03.2B
Substantial	The CSP shall only provide access to or disclose CSC 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.	INQ-03.1S
	The CSP shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate.	INQ-03.2S
	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 CSCs who are subject of the investigation request.	INQ-03.3S
High	The CSP shall only provide access to or disclose CSC 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.	INQ-03.1S
	The CSP shall document and implement procedures to ensure that government agencies only have access to the data they need to investigate.	INQ-03.2S
	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 CSCs who are subject of the investigation request.	INQ-03.3S
	The CSP shall automatically monitor the accesses performed by or on behalf of investigators as determined by the process described in INQ-01.	INQ-03.4H

A.21.3.3 Guidance requirements

- Ultimately, when both data limitation and anonymisation are impossible, the assessment of the investigative request should conclude that the request is to be challenged.

A.22 PRODUCT SECURITY

PROVIDE APPROPRIATE MECHANISMS FOR CLOUD CUSTOMERS.

A.22.1 PSS-01 Error Handling and Logging Mechanisms

A.22.1.1 Objective

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

A.22.1.2 Requirements

Basic	The CSP shall offer to their CSCs mechanisms for error handling, logging and reporting that allow them to obtain security-related information about the status of the <u>cloud service</u> as well as the data, <u>services</u> or functions it provides.	PSS-01.1B
Substantial	The CSP shall offer to their CSCs mechanisms for error handling, logging and reporting that allow them to obtain security-related information about the status of the <u>cloud service</u> as well as the data, <u>services</u> or functions it provides.	PSS-01.1S
	The information provided shall be detailed enough to allow CSCs to check the following aspects, insofar as they are relevant to the CSC's use of the <u>cloud service</u> : and the CSC's assets, such as <u>CSC data</u> , in the <u>cloud service</u> : <ul style="list-style-type: none"> Which data, services or functions available to the CSCs within the <u>cloud service</u>, have been accessed by whom and when (Audit Logs); CSP processing malfunctions for both automatic or manual actions; and Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. 	PSS-01.2S
	The logged information shall be protected from unauthorised access and modification and can be deleted by the <u>CSC</u> .	PSS-01.3S
	When the <u>CSC</u> is responsible for the activation or type and scope of logging, the <u>CSP</u> shall provide appropriate logging capabilities.	PSS-01.4S
	The <u>CSP</u> shall make the <u>information</u> available to <u>CSCs</u> via documented interfaces that are suitable for further processing this information as part of the <u>CSC's</u> Security Information and Event Management (SIEM).	PSS-01.5S
High	The CSP shall offer to their <u>CSCs</u> mechanisms for error handling, logging and reporting that allow them to obtain security-related information about the status of the <u>cloud service</u> as well as the data, <u>services</u> or functions it provides.	PSS-01.1H
	The information provided shall be detailed enough to allow <u>CSCs</u> to check the following aspects, insofar as they are relevant to the <u>CSC's</u> use of the <u>cloud service</u> and the <u>CSC's</u> assets, such as <u>CSC data</u> , in the <u>cloud service</u> : <ul style="list-style-type: none"> Which data, services or functions available to the <u>CSCs</u> within the <u>cloud service</u>, have been accessed by whom and when (Audit Logs); CSP processing malfunctions for both automatic or manual actions; and Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. 	PSS-01.2H
	The logged information shall be protected from unauthorised access and modification and can be deleted by the <u>CSC</u> .	PSS-01.3H
	When the <u>CSC</u> is responsible for the activation or type and scope of logging, the <u>CSP</u> shall provide appropriate logging capabilities.	PSS-01.4H
	The <u>CSP</u> shall make the <u>information</u> available to <u>CSCs</u> via documented interfaces that are suitable for further processing this information as part of the <u>CSC's</u> Security Information and Event Management (SIEM).	PSS-01.5H

A.22.1.3 Guidance requirements

- Deletion is normally managed by the CSC, but the CSP may automatically delete logs after a delay (that should be agreed with the CSC).
- When the CSC gets information through documented interfaces, they may need to pre-process it before feeding it into their own SIEM

A.22.2 PSS-02 Session Management

A.22.2.1 Objective

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

A.22.2.2 Requirements

Basic	A state-of-the-art session management system shall be used that is suitably protected against known attacks.	PSS-02.1B
Substantial	A state-of-the-art session management system shall be used that is suitably protected against known attacks.	PSS-02.1S
	The session management system shall include mechanisms that invalidate a session after it has been detected as inactive.	PSS-02.2S
	If inactivity is detected by time measurement, the time interval shall be configurable by the CSP or – if technically possible – by the CSC.	PSS-02.3S
High	A state-of-the-art session management system shall be used that is suitably protected against known attacks.	PSS-02.1S
	The session management system shall include mechanisms that invalidate a session after it has been detected as inactive.	PSS-02.2S
	If inactivity is detected by time measurement, the time interval shall be configurable by the CSP or – if technically possible – by the CSC.	PSS-02.3S

A.22.2.3 Guidance requirements

- The guidance will need to clarify the notion of “suitable” and “state-of-the-art”.
- Time intervals should be provided by the CSC whenever possible, and the CSP should not override it unless there is a security issue (e.g. infinite time interval, but it is preferable to forbid some values).
- 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

A.22.3 PSS-03 Images for Virtual Machines and Containers

A.22.3.1 Objective

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

A.22.3.2 Requirements

Basic	<p>The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service:</p> <ul style="list-style-type: none"> • The CSC can restrict the selection of images of virtual machines or containers, so that users of this CSC can only launch the images or containers released according to these restrictions. • Images made available by the CSP to the CSC are labelled with information about their origin (CSP or other interested party). • Images originating from the CSP are hardened according to generally accepted industry standards. 	PSS-03.1B
-------	--	-----------

Substantial	<p>The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service:</p> <ul style="list-style-type: none"> The CSC can restrict the selection of images of virtual machines or containers, so that users of this CSC can only launch the images or containers released according to these restrictions. Images made available by the CSP to the CSC are labelled with information about their origin (CSP or other interested party). Images originating from the CSP are hardened according to generally accepted industry standards. 	PSS-03.1S
High	<p>The CSP shall ensure the following aspects if CSCs operate virtual machines or containers with the cloud service:</p> <ul style="list-style-type: none"> The CSC can restrict the selection of images of virtual machines or containers, so that users of this CSC can only launch the images or containers released according to these restrictions. Images made available by the CSP to the CSC are labelled with information about their origin (CSP or other interested party). Images originating from the CSP are hardened according to generally accepted industry standards. <p>An integrity check shall be performed and automatically monitored to detect image manipulations at start-up and runtime of virtual machine or container images, and reported to the CSC</p>	<p>PSS-03.1H</p> <p>PSS-04.2H</p>

A.22.3.3 Guidance requirements

- The images “provided by the CSP” are reference or baseline images that the CSP provides as a service to its customers, and the requirement to inform the CSCs about changes only applies to such images, not to CSC images stored in backup or elsewhere.

A.22.4 PSS-04 Choice of Locations for Data Processing and Storage

A.22.4.1 Objective

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

A.22.4.2 Requirements

Basic	None.	
Substantial	<p>Within the constraints of system availability, the CSP shall allow the CSC to select from available locations (location/country) offered by the CSP for CSC data processing and storage including data backups according to the contractually available options.</p> <p>All CSP commitments regarding locations of CSC data processing and storage shall be supported by technical measures in the cloud service architecture.</p>	<p>PSS-04.1S</p> <p>PSS-04.2S</p>
High	<p>Within the constraints of system availability, the CSP shall allow the CSC to elect from available locations (location/country) offered by the CSP for CSC data processing and storage including data backups according to the contractually available options.</p> <p>All CSP commitments regarding locations of CSC data processing and storage shall be enforced by the cloud service architecture.</p>	<p>PSS-04.1H</p> <p>PSS-04.2H</p>

A.22.4.3 Guidance requirements

- 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

POLITICO

B.1 INTRODUCTION

B.1.1 Purpose

As mentioned in the EU Cybersecurity Act, the conformity assessments performed in the context of the EUCS shall follow the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT services.

The harmonized standard related to the certification of ICT services for Regulation (EC) 765/2008 is ISO/IEC 17065:2012 [ISO17065]. Among the requirements defined for CABs in that standard, many are related to the methodology to be applied by the CAB during a conformity assessment. These methodological elements are generic, and the EUCS defines more specific requirements related to the conformity assessment of cloud services.

In particular, specific requirements are provided related to the EUCS' different evaluation levels, and to the activities related to the assessment of the subservice providers involved in the provision of a cloud service, which shall be applied by the EUCS CABs. In addition, the conformity assessment for the EUCS has been specifically designed to allow the audit activities to be shared with other assessments, including other conformity assessments based on the ISO 17000 series, such as assessments related to the ISO/IEC 27001 requirements on Information Security Management Systems, as well as audits based on the ISAE methodology, derived from financial audits and used in ISAE3402 or SOC2 audits and other kinds of assurance engagements.

The present Annex introduces the overall methodology, and the two following annexes introduce the measures that are specific to the different EUCS evaluation levels.

B.1.2 Definitions

Audit

In the 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.

Assurance

Different definitions of assurance are provided in [ISO/IEC 15408-1] and in [ISO/IEC/IEEE 15026-1], which we have combined as follows:

- grounds for justified confidence that a product, service or process meets specified requirements

Note that auditing standards (including ISO/IEC/IEEE 15026-1) typically refer to claims or assertions made by the customer, whereas certification-related standards, like ISO/IEC 15408-1, refer to requirements. Because the EUCS is a certification scheme, we have made the choice to refer to specified requirements.

Reasonable assurance

A reasonable assurance engagement²⁹ is defined in [ISAE3000] as:

An assurance engagement in which the practitioner³⁰ 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 claim³¹) is *materially misstated*, i.e., contains inaccurate information to a level that has significant consequences on the overall goal. 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, for instance: "Based on the activities performed, in our opinion, the cloud service XYZ satisfies the certification requirements of the EUCS at assurance 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 audit team collects less evidence than for a reasonable assurance engagement but sufficient for a negative form of expression of the audit team's conclusion. The practitioner achieves this ordinarily by performing different or fewer activities than those required for reasonable assurance or using smaller sample sizes for the activities performed.

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 certification requirements of the EUCS at assurance level CS-EL1."

Determination activities

In the conformity assessment of a cloud service, most determination activities are audit activities, and the following ones 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.

²⁹ An audit performed in the context of the EUCS scheme is a kind of assurance engagement.

³⁰ Auditor

³¹ In the case of the EUCS, the management claim is required to include a claim of compliance to all requirements defined in the EUCS, so the assurance engagement effectively covers the fulfilment of the EUCS requirements.

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 the 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.

Reperformance 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.

Reperformance of programmed processing

Input test data, manually calculated expected results, and compared actual results of processing to expectations.

B.1.3 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/IEC 27001 in the form of a table that outlines which of the controls in ISO/IEC 27001's Annex A are applicable and references to further documentation about the applicable controls) or a description about the service-related system of internal controls (e.g., attestations based on 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, the criteria are outlined in form of security objectives and related service requirements, and the applicable criteria are listed in Annex A: (Security Objectives and requirements for Cloud Services). They represent the mandatory baseline per evaluation level for which the CSP shall demonstrate compliance.

In addition, in the EUCS, applicability shall be strict. The service requirements are generic and technology-independent, and they are presumed to be applicable, unless they can practically not be applied (e.g., if a requirement focuses on a cloud capabilities type that is not provided by the cloud service). Nevertheless, the EUCS follows a risk-based approach; depending on the level of risk associated to a given security control, the demonstration of the fulfilment of related service requirements may require more or less evidence.

CSPs may map their internal controls per applicable security control objective and related service requirements. Re-using existing descriptions can limit additional efforts for the CSPs and contribute to the fast adoption of the EUCS. It also allows the CSPs to demonstrate compliance with multiple assurance standards and criteria catalogues during a single conformity assessment (“test once, rely often”). However, this requires the mapping to be complete, accurate and valid. Further, the nature, timing and extent of evaluation activities applied by the CAB must provide the required level of evidence.

B.1.4 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, the CSP shall identify the subservice providers and apply the relevant procedures outlined below.

ASSESSMENT METHODS

The assessment shall consider all subservices listed in the description of the cloud 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 subservice provider in the audit scope (inclusive method);
2. Exclude the subservice provider from the audit scope (carve-out method).

Both methods are dealing with the services provided by a subservice provider, whereby the CSP's description of its service presents the nature of the services provided by a subservice provider. In both cases, internal and external subservices are treated similarly and considered as provided by subservice providers.

Inclusive method

With the inclusive method the subservice provider's controls to meet the applicable security objectives and the related service requirements shall be included in the CSP's description of its cloud service and control framework. The subservices are part of the scope of the conformity assessment of the CSP's cloud service.

Carve-out method

With the carve-out method the subservice provider's relevant control objectives and related controls are excluded (carved-out) from the CSP's description of its cloud service and control framework. The carved-out subservices are not part of the scope of the conformity assessment of the CSP's cloud service. Instead, the CSP shall define Complementary Subservice Organization Controls (CSOCs) and associated requirements, which describe how the implementation of its own controls rely on those implemented by the subservice provider. The fulfilment of the requirements on CSOCs is not considered in the audit itself, but it shall be considered in the dependency analysis that is performed separately, and which relies on the analysis of assurance information provided by the subservice provider (see section B.8 below).

In addition, the CSP's description shall present those controls that are designed and implemented to monitor the operating effectiveness of the controls at the subservice provider. The monitoring activities shall meet the security objectives and the related service requirements for "Procurement Management (Supply Chain Management)" defined in Annex A: (Security Objectives and requirements for Cloud Services).

SUBSERVICES IN THE EUCS

In the context of the EUCS, subservices assessed using the inclusive method shall simply be considered as part of the scope of the cloud service's conformity assessment. The CSP shall be responsible for ensuring that all required evidence is available about the subservice provider, about the services it provides, and about how these subservices are integrated in its own systems for the provision of the cloud service to be assessed.

Subservices assessed using the carve-out method shall be considered at all stages of the conformity assessment, and in particular during the dependency analysis (see section B.8 below). During that phase, the audit team shall review the assurance information 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.1.5 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 providers operate complementary controls that work in combination with the CSP's internal controls to achieve the EUCS security objectives and related service requirements.

In the EUCS, the CSP shall present the Complementary User Entity Controls (CUECs) and the Complementary Subservice Organization Controls (CSOCs) assumed in the design of its internal controls as part of the description of the cloud service and its control framework.

In addition, the CSP may also be a consumer of CUECs. If the CSP uses a subservice provider, the CSP shall obtain relevant information about the CUECs that the subservice provider assumed in the design of their internal controls, and related requirements. Relevant information can be obtained from the subservice provider, 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, SOC 2 or BSI C5). For these CUECs the CSP shall ensure that appropriate internal controls are in place. During a conformity assessment, the CAB shall evaluate whether the controls related to these CUECs are suitably designed, implemented and, for evaluation levels CS-EL2 and above, operating effectively.

B.1.6 Presentation

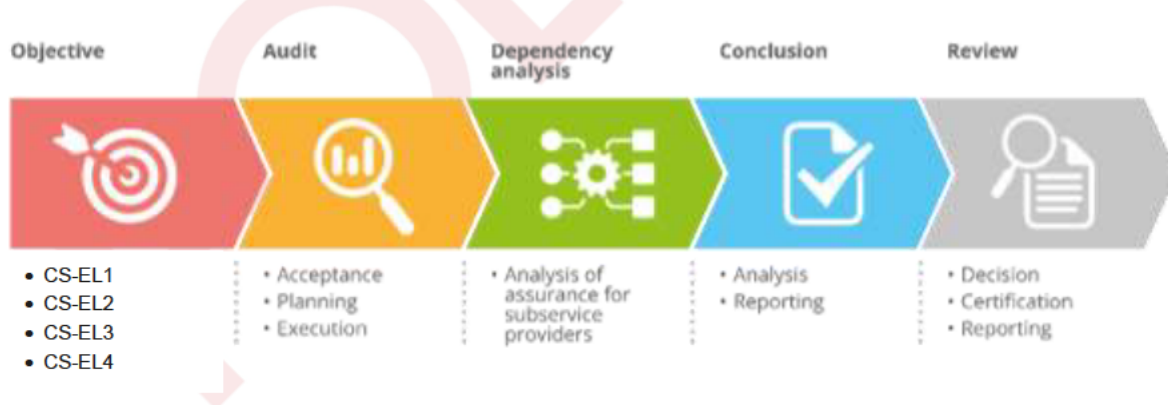
The assessment of cloud services for all evaluation levels of the EUCS shall be based on a meta-approach, which is described here. This meta-approach for assessing and determining conformity describes the overall flow and requirements of the conformity assessment of cloud services in the context of the EUCS scheme.

The meta-approach is the same for all evaluation levels, except for the audit itself:

- For evaluation levels CS-EL2 and above, the CAB shall use an audit approach based on either ISO standards or ISAE standards, 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 CS-EL2 and above).
- For evaluation level CS-EL1, as mentioned in the EUCSA, 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 CS-EL1).

The structure of this meta-approach shall start with defining a clear objective, followed by the development and execution of an audit plan and the execution of a dependency analysis, and ending with the analysis of the gathered evidence and the delivery of an evaluation report.

Figure 3: The structure of the Meta-Approach



There is no specific order in the execution of the audit and of the dependency analysis. A CAB may decide to perform all or part of the dependency analysis at the beginning of the conformity assessment, in particular if there are uncertainties about the quality of the assurance information available from some subservice providers. In practice, the ordering of the activities depends greatly on the organization of the conformity assessment activities by the CAB.

The term “audit” is used for all conformity assessment activities performed by the audit team and audit team leader of the CAB, including the analysis of obtained evidence, the reporting of which is the core of the evaluation report.

To be able to conclude whether all service requirements of the EUCS are met, considering the carve-outs and the use of subservice providers, a separate analysis and evaluation shall take place. This dependency analysis, during which

the audit team and audit team leader, or another team designated by the CAB (nevertheless called “the audit team” for simplification), shall analyse the assurance information available for the CSP’s subservice providers, and provide the results in the evaluation report in addition to the audit report.

The evaluation report shall form the basis for awarding a certificate, after review by a team of the CAB independent from the audit team, and together with the delivery of a certification report.

Following [ISO17065], the CAB that issues a certificate shall perform the review and decision activities internally, using its own resources. However, other activities may be subcontracted, and in particular the audit. Throughout this documentation, the audit team may therefore be part of the CAB or of a subcontractor to the CAB. In all cases, requirements applicable to CABs also apply to their subcontractors, in particular regarding the required competences.

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 EUCS certification requirements, including the security objectives and related service 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 cloud service that outlines the underlying and supporting processes and the accompanying statement from the CSP’s top management about the conformity of their cloud service with the certification 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 service 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 CS-Basic level

The objective is to provide limited assurance through the execution of an audit (evaluation) by an independent audit team that the cloud service is designed to fulfil the EUCS certification requirements, including the security control objectives and related service requirements as defined in the EUCS that are applicable to evaluation level CS-EL1.

The audit team shall obtain sufficient and appropriate evidence by executing audit activities as defined in Sections B.3, B.5 and D.3 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 service requirements as defined in the EUCS; and
- the existence and implementation of these controls as of a specified date during the conformity assessment.

B.2.3 CS-Substantial Level

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent audit team that the cloud service is built and operated with procedures and mechanisms to fulfil the EUCS certification requirements, including the security control objectives and related service requirements as defined in the EUCS for the evaluation level CS-EL2.

The audit team shall obtain sufficient and appropriate evidence by executing audit activities as defined in Sections B.3, B.5 and C.3 about:

- the information presented in the description as provided together with or embedded in the application (B.3);
- the suitability of the design of controls to meet the security control objectives and related service requirements (C.3.1);
- the existence and implementation of these controls as of a specified date during the initial conformity assessment (C.3.2); and
- the operating effectiveness (consistent application) of these controls throughout a specified period (C.3.3).

B.2.4 CS-High levels

The objective is to provide reasonable assurance through the execution of an audit (evaluation) by an independent audit team that the cloud service is built and operated with procedures and mechanisms to fulfil the EUCS certification requirements, including the security control objectives and related service requirements as defined in the EUCS for the evaluation levels CS-EL3 and CS-EL4.

The audit team shall obtain sufficient and appropriate evidence by executing audit activities as defined in Sections B.3, B.5 and C.3 about:

- the information presented in the description as provided together with or embedded in the application (B.3);
- the suitability of the design of controls to meet the security control objectives and related service requirements (C.3.1);
- the existence and the implementation of these controls as of a specified date during the initial conformity assessment (C.3.2);
- the operating effectiveness (consistent application) of these controls throughout a specified period (C.3.3); and
- the resistance of the cloud service against attacks performed by skilled attackers (C.3.4).

B.3 APPLICATION AND APPLICATION REVIEW

The CSP shall provide an application document for EUCS certification to the CAB of their choice, provided that the CAB meets the accreditation, notification and where applicable authorisation criteria according to the evaluation level targeted, following the template defined in Section F.2 (Application document).

Then, the CAB shall conduct a review of the information provided by the CSP to ensure that:

- the application document contains all the information mandated by EUCS;
- the scope of certification is clearly defined;
- when applicable, the CSP has provided evidence that it meets all eligibility requirements, as defined in Annex J: (Protection of European data against unlawful access);
- the information about the CSP and the cloud service is sufficient for conducting the assessment and the certification process;
- the CSP has acknowledged and understands its responsibilities as defined in EUCS;
- any known difference in understanding between the CAB and the CSP is resolved, including agreement regarding standards or other normative documents;
- the means are available to the CAB to perform all evaluation activities, including the required resources, capabilities and competences are available to the CAB to perform the conformity assessment, 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 CSP shall also provide the following information:

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

In addition, the audit team 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 cloud service ("Description"), and accompanying CSP's assertion ("Management Statement");
- the CSP is responsible for ensuring that the certified cloud service continues to fulfil the certification requirements during the validity period of the certificate;
- 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 that are consistent with the scope of certification;
- the CSP does not use the certification of its cloud service in such a manner as to bring the CAB into disrepute and does not make any statement regarding the certification of its cloud service that the CAB may consider misleading or unauthorized.

In addition, if the conformity assessment is not an initial conformity assessment, the CSP shall also describe:

- the nature of the maintenance conformity assessment ('surveillance', 'recertification' or 'special');
- the reason for the maintenance conformity assessment;
- the changes in the cloud service and in the CSP's control framework since the last conformity assessment, and the impact of these changes on the certification.

B.4 AUDIT PLAN DEVELOPMENT

The CAB shall plan the conformity assessment 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 activities 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 evaluation level.

During this phase, the CAB shall:

- a) determine the audit objectives, scope and criteria;
- b) select and appoint the audit team;
- c) determine the audit time.

The audit criteria shall be used as reference against which conformity is determined, and shall include:

- the EUCS service requirements defined in Annex A: (Security Objectives and requirements for Cloud Services) for the targeted evaluation level;
- when applicable, the requirements listed in the extension profiles to which the CSP has claimed compliance in the application document;
- if the CSP has declared subservice providers, the CUECs defined for the services provided by these subservice providers in the operation of the cloud service;
- the defined processes and documentation of the service operated by the CSP, and of its associated controls.

The audit criteria focus primarily on the EUCS service requirements, and there is no obligation to consider the other certification requirements, which are defined in the scheme itself (e.g., the notification of the CAB for some vulnerabilities and security incidents). Compliance to these requirements is primarily enforced through other means, in particular the NCCA's surveillance activities. Nevertheless, CABs should be aware of these certification requirements in order to identify potential non-compliance of the CSP to their obligations related to their certified cloud services when they perform maintenance conformity assessments. ENISA may define additional guidance on this topic, in collaboration with the ECCG.

In order to develop the audit plan, the audit team shall:

- a) obtain an understanding of how the CSP's cloud service and associated controls meet the audit criteria;
- b) assess, if applicable, the mapping between the audit criteria, including the EUCS service requirements, and the CSP's control framework
- c) determine to what extent and for which elements of the CSP's internal controls subservice providers are being used and how the CSP controls and monitors the services provided by these subservice providers;
- d) assess how the CSP has defined complementary controls towards its customers (CUEC) and towards subservice providers (CSOC);
- e) assess how the CSP meets requirements on complementary controls of its own subservice providers towards the CSP.
- f) consider 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, the existence of controls and, for evaluation levels CS-EL2 and above, the operating effectiveness of controls, primarily based on qualitative factors, for example: whether the description includes the significant aspects of the service in accordance with the requirements as defined by the EUCS; whether the description omits or distorts relevant information;
- g) determine the audit activities needed to obtain sufficient and appropriate objective evidence about the design, implementation and operating effectiveness of the CSP's cloud service and related controls to meet the audit criteria, including the EUCS service requirements, and describe them in the audit plan.
- h) determine the roles and responsibilities of the audit team members, as well as guides and observers or interpreters;
- i) determine the logistics and communications arrangements, including specific arrangements for the locations to be audited (e.g., datacentre visits);
- j) determine matters related to confidentiality and information security of records obtained during the audit;
- k) determine any follow-up actions from a previous audit or other source(s) e.g., lessons learned, project reviews.

In the case of a surveillance, re-certification or special audit, as specified in Annex G: (Certification Life cycle and continued assurance), the audit team shall also:

- a) analyse the impact assessment provided by the CSP 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 conformity assessment;
- b) analyse the type of audit, and when applicable, the rationale for the audit, to determine the subset of audit activities that need to be performed in order to satisfy the specific requirements for that audit.

In all cases, and for all evaluation 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 evaluation level CS-EL1 is provided in section D.2 and additional information specific to evaluation levels CS-EL2 and above is provided in section C.2.

B.5 EXECUTION

In the execution phase the audit team shall obtain sufficient and appropriate evidence regarding:

- the suitability of the design of controls, including controls over the processes outsourced to subservice providers (such as hosting, infrastructure, platform, etc.) to meet the audit criteria, including the EUCS service requirements;

- 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 CS-EL2 and above assurance levels, the operating effectiveness of the implemented controls throughout a period over time (specified period);

Additional information specific to evaluation level CS-EL1 is provided in section D.3 and additional information specific to evaluation levels CS-EL2 and above is provided in section C.3. The audit team shall document the activities executed, the evidence gained and conclusions reached using the appropriate document (depending on the evaluation level).

Figure 4: The structure of the Meta-approach



B.6 ANALYSIS OF RESULTS

Once the audit team has gathered all required evidence, the audit team shall evaluate its sufficiency and appropriateness. This part of the process is specific to every evaluation level, with the exception of nonconformity handling, which is common to all evaluation levels and is described below.

Additional information specific to evaluation level CS-EL1 is provided in section D.4 and additional information specific to evaluation levels CS-EL2 and above is provided in section C.4.

B.6.1 Nonconformity handling

If the audit activities reveal nonconformities in the design, or if required, operation of the controls, the audit team shall determine whether the applicable audit criteria, and in particular the EUCS service requirements, were still met. The audit team should consider the following activities for the determination:

- Notification of the CSP if the nonconformity has been identified by the audit team;
- Inquiry regarding the CSP's 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 nonconformity as minor or major;

These activities 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, the audit team 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 audit team shall 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 nonconformity, 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 service 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 audit criteria, including the EUCS service requirements, which have not been considered in the design of this audit criterion (e.g., use of new technical measures that provide at least an equal level of security but that are not prescribed in the EUCS service requirements). Compensating controls are also considered a temporary measure, and nonconformities, even minor, are expected to be corrected in the following conformity assessments. The audit team may therefore define a list of conformity assessment activities to be performed in subsequent conformity assessments.

For a major nonconformity, the audit team shall 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 controls 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. In such a case the CAB shall consider both nonconformities separately.

The definition of minor and major nonconformities as well as the requirements related to their handling may be refined in guidance provided by ENISA in collaboration with 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 evaluation 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 evaluation 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 evaluation.
- The corrective actions to remedy the nonconformity in the future and when these measures are likely to be completed or effectively implemented.

If nonconformities have been identified, the audit team 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 audit team shall report nonconformities even if, on the basis of tests performed, they have concluded that the related audit criteria were met, and even if the CSP has implemented corrective actions to address the nonconformities and the audit team has determined that the corrective actions effectively address the nonconformities.

B.7 ISSUING THE PARTIAL EVALUATION REPORT

After evaluating the result of the audit activities, the audit team shall form an audit conclusion and issue a first version of the evaluation report, pending the results of the dependency analysis, that satisfies the requirements defined in Annex F: (Scheme Document Content requirements), section F.4.1, for the targeted evaluation level.

The conclusion shall include the auditor's recommendation as to whether the cloud service satisfies audit criteria, including the EUCS service requirements, pending the results of the dependency analysis. The audit conclusion shall be based on the audit findings, on the objective evidence obtained and the audit activities performed.

This evaluation report shall be first addressed to the CSP. The CSP may contest the content of the evaluation 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.

Note that there is no obligation to perform the dependency analysis independently of the main audit. The two activities may be mixed, and the CAB may then issue directly a full evaluation report, as described in section B.9)

B.8 PERFORMING THE DEPENDENCY ANALYSIS

B.8.1 Objectives

The objective of the dependency analysis shall be to validate that the assurance information (assurance reports, evaluation reports, certificates, or other) available for the subservices operated by internal or external subservice providers used by the CSP in the operation of its cloud service are adequate.

For every subservice, the basis for this dependency analysis is the risk assessment of the subservice provider that has been performed by the CSP. As required by EUCS (see Annex A: Security Objectives and requirements for Cloud Services), the evaluation report shall contain a rationale explaining how the CSP uses the subservice to satisfy the audit criteria, including the EUCS service requirements, and for each subservice a pointer to assurance information for the subservice.

The dependency analysis consists in analysing this assurance information to determine whether or not the subservice meet the expectations from the CSP at the targeted evaluation level.

B.8.2 Assessing the availability of assurance information

The first step is to list the assurance information available for every subservice provider, and to assess the overall relevance of each assurance information document for the dependency analysis.

The following elements are essential for each assurance information document.

About the document itself:

- Type of document, with all required details (e.g., ISO27001 certificate or evaluation report, 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 as part of the assurance information;

About the audit team's professional competence and independence:

- Name of the CAB or audit organization, name of the audit team leader.
- Evidence of the CAB/audit organization's and the auditors' competence (accreditation, authorization, personal certification, etc.).
- Evidence of the CAB/audit organization's and the auditors' independence (accreditation, etc.).

By analysing this information, the audit team shall determine whether the assurance information available for a given subservice provider is adequate to provide assurance corresponding to the targeted EUCS evaluation level.

ENISA, in collaboration with the ECCG, will issue guidance about the acceptability of different types of assurance information documents for the different EUCS evaluation 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 information available for the subservice provider is adequate to determine that the subservice provider meets the expectations of the CSP relative to individual audit criteria, such as service requirements defined in the EUCS.

This assessment is performed for every subservice provider, and then for every audit criterion for which the CSP has declared to rely partially or fully on the assurance information provided by the subservice provider, by formulating an assumption on the subservice's control.

The assumptions on subservice providers cover both the security of the services they provide and their contribution to the security of the CSP's cloud service. These assumptions should be mapped to CSOCs and to requirements on these CSOCs.

The audit team shall determine for each such CSOC and requirement whether or not the assurance provided in the available assurance information is adequate. There are several ways to reach a conclusion that the assurance is adequate:

- The required information is available with the expected level of assurance in the assurance information.
- The information available in the assurance information 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 audit team to determine that the information is adequate.
- The information available in the assurance information does not offer the expected level of assurance, but the controls implemented by the CSP to assess and monitor the subservice provider allow the audit team to determine that the information is adequate.

Finally, if the assurance information mentions nonconformities on the controls used to meet an assumption, the corrective measures proposed and implemented by the subservice provider and reviewed by its audit team shall be adequate to guarantee that the requirements related to that assumption are indeed met.

ENISA, in collaboration with the ECCG, will issue guidance about the adequacy of different types of assurance information documents for the different evaluation levels supported by EUCS, 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 is a cloud service that has been certified in the EUCS scheme, the processes defined above may be simplified:

- The audit team's competence and independence does not need to be assessed;
- The evaluation report and certification report can be considered as being fully compliant with the rules of the EUCS for the evaluation level of the report;
- No mapping to the EUCS service 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 provider has already been assessed.

B.9 ISSUING THE EVALUATION REPORT

After evaluating the results of the evaluation activities, and after evaluating in the dependency analysis the adequacy of the assurance provided to support assumptions about subservice providers, the audit team shall form a final

conclusion and issue an evaluation report that satisfies the requirements defined in section F.4 (Evaluation report) for the targeted evaluation level.

The conclusion shall include the auditor's recommendation as to whether the cloud service satisfies the audit criteria, including the EUCS service requirements. The conclusion shall be based on the objective evidence obtained and on the audit activities performed.

The conclusion shall include the audit team's recommendation as to whether the assurance information available about the CSP's subservice providers is adequate or not to support the certification of the cloud service that relies on these subservice providers. The conclusion shall be based on the results of the activities performed during the dependency analysis and express whether, in all relevant aspects,

- (i) the assurance information provided for every subservice provider is adequate to provide assurance corresponding to the targeted EUCS evaluation level,
- (ii) for every CSOC and requirement on CSOC formulated by the CSP regarding a contribution of a subservice provider to the conformity to an audit criterion, the audit information provided for that subservice provider is adequate to determine that requirement on the CSOC formulated by the CSP is fulfilled, with the targeted EUCS evaluation level, and
- (iii) for every nonconformity identified in assurance information regarding a control used to determine that an assumption formulated by the CSP is correct, appropriate corrective actions, or in the case of a minor nonconformity, compensating controls, have been proposed, implemented and validated by an audit team.

The audit team shall then combine the partial conclusions on evaluation activities and on dependency analysis, for a conclusion regarding the fulfilment of relevant audit criteria, and in particular of EUCS service 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 document.

This evaluation report shall be first addressed to the CSP. The CSP may contest the content of the evaluation report and in particular the auditor'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 audit team then delivers the evaluation report, and if applicable, additional assurance or evaluation reports of subservice providers, to the CAB accredited to issue EUCS certificates, which will then proceed to a review and certification decision.

B.10 REVIEW OF THE EVALUATION

Once an evaluation report (and, if required, supporting reports) has been delivered by the audit team, 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 evaluation process, 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;

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.

If the certification decision is negative, *i.e.*, if the cloud service has been determined not to meet the certification requirements of the EUCS, 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, and then the process for handling nonconformities shall be followed.

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.

If the certification decision is positive, *i.e.* if the cloud service has been determined to meet the certification requirements of the EUCS, the consequences are as follows, depending of the nature of the conformity assessment.

- In the case of an initial conformity assessment, the CAB shall issue a new certificate, and set the expiry 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 surveillance conformity assessment, the CAB shall update the existing certificate by indicating the date of the surveillance conformity assessment, and if needed by updating elements in the certificate that have changed;
- In the case of a re-certification conformity assessment, the CAB shall update the existing certificate by setting the expiry date of the certificate three (3) years after the date of this update, unless the CAB has explicitly indicated a shorter validity period for the certificate, and if needed by updating elements in the certificate that have changed;
- In the case of a special conformity assessment following the suspension of a certificate, the CAB shall update the existing certificate if needed by updating elements in the certificate that have changed, and shall return the certificate's status to 'certified';

Certificates shall contain the information listed in Chapter 17 (Certificate Format).

B.12 CERTIFICATION DOCUMENTATION

Following every positive certification decision, a certification report shall be appended to the certificate, following the requirements defined in section F.6.2, Certification report.

ANNEX C: ASSESSMENT FOR LEVELS CS-EL2 AND ABOVE

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

POLITICO

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 CS-EL2, CS-EL3 and CS-EL4 evaluation 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 on the development of the audit plan, its execution, and the analysis of the audit results.

C.2 DEVELOPING THE AUDIT PLAN

The audit plan shall describe audit activities ³²specifically suited for the specific audit to be performed. The audit team shall ensure in the definition of the audit activities that they are adapted to the specific risks that prevent the CSP from meeting the certification requirements of the EUCS and applicable standards, considering at least:

- a) the cloud service provided by the CSP;
- b) the components of the systems used to provide the cloud service;
- c) the environment in which these systems operate.

In their consideration of the risks associated to the CSP's cloud service and controls, the audit team shall tailor the audit activities to the specific circumstances by considering the following aspects:

- a) the competence of the personnel in charge of implementing the controls;
- b) the relevance and reliability of the evidence to be obtained;
- c) the nature of the controls, including their level of automation, and the frequency with which they operate;
- d) the degree to which the controls rely on the effectiveness of other controls.

If the audit is not an initial audit, the audit team shall consider additional aspects:

- a) changes to the systems used to operate the cloud service or to the CSP, including but not limited to the changes in the cloud service and its controls declared by the CSP;
- b) changes in key personnel;
- c) the history of errors in operation of the controls, as well as the history of nonconformities, as known from previous audits;

In addition, the audit team shall consider the evaluation level targeted for certification.

Based on all the parameters above, the audit team shall determine for each audit activity:

- a) the nature (what kind of audit activity);
- b) the timing (at what point in time or over what period);
- c) the extent (how many times or how often to execute the activity).

The nature of the audit activity shall be one of the audit activity types: inquiry, observation, inspection, reperformance of monitoring activities or manual controls and reperformance of programmed processing.

The timing of the audit activity shall define the point in time or the period to be covered by an audit activity:

- a point in time shall be specified for audit activities related to the design, implementation and existence of a control;

³² Determination activities may include additional activities, including in particular vulnerability identification activities; however, this chapter focuses solely on audit activities.

- a period shall be specified for audit activities related to operating effectiveness, typically covering the period since the last audit, or for an initial certification audit, a period preceding the audit, as defined below.

The extent of the audit activity shall provide a quantitative or qualitative aspect to the audit activity, such as:

- the number of observations to be performed;
- the rigour and depth of inquiries;
- the number of documents or other evidence to be inspected;
- the number of reperformances for a specific audit activity.

The extent shall be determined from the specific characteristics of the control being audited, and from the evaluation level required.

In many cases, and in particular for assessing operating effectiveness over a period of time, a sampling approach shall be used. The sample size for a given frequency shall be chosen considering the nature of the audit activity and the targeted evaluation level.

Alternative or complementary information on sample sizes may be provided in harmonized guidance provided by ENISA in collaboration with the ECCG or in standards or Technical Specifications.

In determining the nature, timing and extent of the assessment, the audit team shall consider:

- a) the nature and frequency of the controls being evaluated,
- b) the types of available evidence,
- c) the nature of the requirements to be met;
- d) the assessed level of control risk,
- e) the expected efficiency and effectiveness of the audit activities,
- f) the results of the audit activities of the control's environment.

The audit plan shall include a description of the audit activities, including for each audit activity:

- a) an identification of the control under audit;
- b) the nature of the audit activity;
- c) the timing of the audit activity;
- d) the extent of the audit activity;

After execution of the audit, the information for every audit activity shall be complemented with:

- a) the documents used, the names and function of the inquired persons, and other information about execution of the audit activity;
- b) the audit evidence obtained;
- c) the conclusion reached, as an audit finding.

The information in the audit plan, including the information added after the execution of the audit, and including any document pointed to that the audit team has a copy of, shall be archived by the CAB according to the requirements defined in the EUCS regarding record retention. This information shall also be the basis for the development of the evaluation report.

The audit activities shall be tailored to every audit, depending, among other things, on the requested evaluation level, and the audit team's judgement, including the assessment of the risks of impactful nonconformity of the matter being investigated.

C.3 AUDIT EXECUTION

During this phase, the audit team shall perform the audit activities to evaluate the cloud service, in accordance with the audit plan and including the suitability, existence and operating effectiveness of the controls associated to the provision of the cloud service.

At levels CS-EL3 and CS-EL4, the CAB shall also evaluate the resistance of the cloud service against skilled attackers.

C.3.1 Suitability of the design of controls

A control is suitably designed when actions or events that comprise a risk are prevented, or detected and corrected. In order to obtain evidence regarding the suitability of the design of controls, the audit team shall determine whether

- The risks that threaten the achievement of the audit criteria, including EUCS service requirements, have been identified by the CSP;
- The controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the audit criteria, including EUCS service requirements, from being fulfilled.

To be able to conclude on this, the audit team shall:

- a) obtain an understanding of the CSP's process for identifying and evaluating the risks that threaten the fulfilment of the audit criteria, including EUCS service requirements and assessing the completeness and accuracy of the CSP's identification of those risks;
- b) 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);
- c) evaluate the party responsible for conducting the control (e.g., competence and authority of the person, group or system);
- d) 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;
- e) 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 audit team to inquire the CSP's subject matter experts and to inspect supporting documentation that describe how the control should operate, e.g., written policies, procedures or process flowcharts.

C.3.2 Existence of an implementation of controls

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 audit team has concluded that a control is suitably designed, the next step is to verify that the control actually exists and is implemented as designed.

To be able to conclude on this, the audit team shall obtain evidence that the controls have been implemented by examining exemplary actions or events that triggered the occurrence or performance of the controls (e.g., tickets) and inspecting 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.3.3 Operating effectiveness

Controls considered to be suitable in design shall be audited for operating effectiveness over a specified period. The audit team shall design the audit activities 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 an initial conformity assessment, the specified period shall be 6 months for evaluation level CS-EL2 and 12 months for evaluation levels CS-EL3 and CS-EL4. For subsequent conformity assessments the specified period shall cover 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.

If a control is new or has been modified during that specified period, the audit team shall record that operating effectiveness was not assessed on the current version of the control for the full specified period. This may lead to a nonconformity if the audit team's judgment is that the available information and the extent of changes do not allow them to assess whether audit criteria mapped to this control, including EUCS service requirements were fulfilled throughout the specified period.

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 audit team shall perform activities such as document inspection, or reperformance in combination with inquiries to obtain evidence about the following:

- a) how the control was applied;
- b) the consistency with which the control was applied;
- c) by whom or by what means the control was applied.

An inquiry alone is not sufficient to determine whether a control operated effectively throughout the specified period. This assessment of operating effectiveness shall apply to all controls, including, if applicable, to controls over the CSP's processes and to controls that are outsourced to subservice providers.

At evaluation levels CS-EL3 and CS-EL4, in addition to the evaluation of operating effectiveness, the CSP shall define procedures, validated by the audit team, for the automated monitoring of essential security controls, as specified in the EUCS service requirements and 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 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 monitoring.

Specific EUCS security objectives and the related service requirements define the general requirements for these procedures, and also define the minimum set of automated monitoring mechanisms to be implemented by the CSP.

C.3.4 Resistance against skilled attackers

At evaluation levels CS-EL3 and CS-EL4, the evaluation activities shall include testing activities to be performed by a testing laboratory accredited to ISO/IEC 17025, and authorized by the NCCA. These activities focus on the identification of potential vulnerabilities; they shall include a review of the configuration of the systems providing the cloud service, a review of the cloud service's source code, as well as penetration testing activities.

These activities shall evaluate how the CSP identifies vulnerabilities that may be exploited by such skilled attackers. The evaluation activities performed by the laboratory may cover all the CSP's activities related to the identification of vulnerabilities (e.g., for a small CSP that relies on composition with a certified infrastructure provider), or only a representative subset of the CSP's activities in this area (e.g., for a large infrastructure provider).

ENISA, in collaboration with the ECCG, shall provide harmonized guidance defining a reference set of vulnerability identification activities to be undertaken by CSPs in order to assess the resistance of their cloud service to skilled attackers, as well as guidance on the definition of a representative subset of these activities to be performed by the laboratory.

The result of these vulnerability identification activities, whether performed by the CSP or by the laboratory, shall then be the subject of audit activities by the audit team, including at least an inspection, to assess how they actually meet the objective of protecting the cloud service against skilled attackers, as defined in the EUCS service requirements.

C.4 ANALYSIS OF RESULTS

C.4.1 Evaluation of evidence obtained

The audit team shall evaluate the sufficiency and appropriateness of the evidence obtained from the executed audit activities to conclude about the suitability of the design, existence and implementation, and operating effectiveness of the controls.

The evidence obtained shall be appropriate and sufficient to enable the CAB (including the audit team and the review team) to consider it as audit evidence, used as a basis for audit findings and audit conclusions, and to take informed decisions.

In addition, when using information produced (or provided) by the CSP, the auditor shall assess whether this information is reliable enough for executing the planned audit activities by obtaining evidence about the accuracy and completeness of such information and assessing 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 that the description is not fairly presented and that the controls were not suitably designed and implemented and, if required, operating 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 audit team'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 audit criteria, including applicable EUCS service requirements.

If the audit team is unable to obtain sufficient sufficient and appropriate evidence to conclude on a given requirement, then the audit shall be considered inconclusive. This shall be considered as a nonconformity, and handled as such.

C.4.2 Analysis of controls to meet the audit criteria

The analysis of the suitability of the design, existence and implementation, and operating effectiveness of the CSP's internal controls, shall be based on the requirements outlined in the section above.

For analysing whether the CSP's internal controls meet the audit criteria, including the EUCS service requirements, the audit team shall consider whether the controls fully cover all aspects of the audit criteria. Several controls may need to be combined to fully meet each audit criterion.

If the CSP already performs audits in accordance with other standards (e.g. ISO/IEC 27001 or ISAE 3402), the controls presented in the description may be optimally aligned with the criteria of these standards, but their descriptions may not fully meet all aspects of the audit criteria to which they are mapped.

The audit activities and the results thereof, including audit findings, shall be documented in the evaluation report according to the examples in the table below

Security Control Objectives	<Service-Org>'s Description of Controls	Procedures Performed	Procedure Results
Objective: description			
ID – Audit criterion	ID – Title of Control [Control Description]	Test performed by the auditor	Test result by the auditor

In describing the audit of controls in the evaluation report, the audit team shall clearly state per control tested, whether the items audited represent all or a sample of the items in the population. The audit team shall further indicate the nature of the audit activity in sufficient detail to enable the CAB's review team to review whether the audit team has obtained sufficient and appropriate evidence in accordance with the requirements defined in this annex.

ANNEX D: ASSESSMENT FOR LEVEL CS-EL1

PURPOSE	This annex describes the applicable conformity assessment method for level CS-EL1.
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 8, Evaluation Methods and Criteria

POLITICO

D.1 INTRODUCTION

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.

For the corresponding CS-EL1 evaluation level, the conformity assessment is therefore greatly simplified, as the audit only aims at providing limited assurance. The evidence shall be gathered by focusing on a documentation review of the internal audit performed by the CSP, following a questionnaire defined specifically for the CS-EL1 evaluation level. The CSP shall also provide evidence related to the internal audit, and the CAB shall then review the result of this internal audit and confirm the sufficiency and appropriateness of the accompanying evidence to provide limited assurance.

For the evaluation level CS-EL1 the CAB shall use the approach defined in the present Annex.

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 CS-EL1 evaluation level.

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 on the development of the audit plan, its execution, and the analysis of the audit results.

D.2 DEVELOPING THE AUDIT PLAN

Sufficient and appropriate objective evidence about the design and implementation of the CSP's internal controls shall be obtained through review of the provided documentary evidence and if necessary, by inquires to be able to evaluate the provided documentary evidence in order to determine whether

- a) the evidence addresses the audit criteria, including the EUCS service requirements in a sufficiently comprehensive manner;
- b) the evidence is sufficiently clear and unambiguous in how the requirements are met and how controls have been implemented by the CSP;
- c) the evidence is *prima facie* plausible (i.e., it appears in the professional opinion of the audit team 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 should be achieved by using a harmonized questionnaire to be used by the CSP in their internal audit and associated audit plan.

ENISA, in collaboration with the ECCG, should define such a harmonized questionnaire, together with guidance about its usage in the CSP's internal audit and in the CAB's subsequent review.

D.3 AUDIT EXECUTION

During this phase, the audit team performs the audit activities to evaluate the cloud service, including the suitability and existence of the controls associated to the provision of the service. This stage shall include at least one meeting between the CAB and the CSP at one of the site(s) of the CSP.

The audit team shall obtain sufficient and appropriate audit evidence by evaluating the objective evidence provided by the CSP regarding:

- the suitability of the design of controls, including controls over the outsourced processes (such as hosting, infrastructure, platform, etc.) to meet the audit criteria, including the EUCS service requirements;
- the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date).

The execution of the audit starts when the CSP has provided all required documentation, including the questionnaire with the answers from their internal audit. The audit team shall document the activities executed, the evidence gained and conclusions reached, preferably as a complement to the harmonized questionnaire filled by the CSP.

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 audit team to determine whether

- The risks that threaten the fulfilment of the audit criteria, including the EUCS service requirements, have been identified by management;
- The controls are, if operating effectively, able to prevent or detect audit criteria 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 audit team 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 audit team shall obtain evidence related to exemplary actions or events that triggered the occurrence or performance of the controls (e.g., tickets) and to review 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.4 ANALYSIS OF RESULTS

In forming the conclusions on the evidence obtained the audit team shall

- a) evaluate whether the described technical and organizational controls refer to or describe the applicable certification requirements;
- b) consider whether the provided documents adequately disclose the significant information security policies and the selected and implemented technical and organizational controls;
- c) consider whether the information security policies and technical and organizational controls are deemed suitable to meet the audit criteria, including the EUCS service requirements, considering the nature of the cloud service;
- d) evaluate how the information provided appears relevant, reliable, comprehensive and comparable.

On this basis the audit team shall assess if it can be concluded that

- nothing has come to its attention that causes the audit team to believe that the technical and organizational controls warranted by the CSP are not fulfilling in all relevant aspects the requirements of the CS-EL1 evaluation level in accordance with the EUCS, and that
- the evidence presented is at least sufficient for the audit team to obtain a limited level of assurance.

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

POLITICO

E.1 REQUIREMENTS FOR ALL LEVELS

All CABs that issue certificates or perform audit activities shall be accredited to ISO/IEC 17065, which is the harmonized standard for the certification of products and services, which applies to cloud services. For this accreditation, the ISO/IEC 17065 requirements will be complemented by additional requirements specific to the EUCS, to be defined in a separate document, which will be provided as guidance by ENISA with the support of the ECCG, as a Technical Specification or International Standard by CEN-CENELEC, or as a combination of both.

These documents shall define competence requirements for the various roles in the performance of conformity assessment activities, and they shall include specific requirements related to the conformity assessment of cloud services.

The competences verified in the accreditation process shall be considered sufficient for the issuance of certificates at the CS-EL1 and CS-EL2 evaluation levels.

E.2 ADDITIONAL REQUIREMENTS FOR LEVEL CS-EL3 AND CS-EL4

For CABs that issue certificates or perform audit activities at evaluation levels CS-EL3 and CS-EL4, additional requirements shall be fulfilled, mostly related to the assessment of the EUCS service requirements around vulnerability identification and penetration testing. These requirements are mostly technical and related to testing activities, so the conformance of CABs to these requirements will be verified during the authorization process performed by the NCCA before notifying a CAB to the European Commission.

These requirements mostly apply to the audit team, which means that the competences need to be available in the team, but not by every member of the team. A single auditor or technical expert may be sufficient.

The competences are strongly related to the technical requirements defined in the section on vulnerability identification and penetration testing for evaluation levels CS-EL3 and CS-EL4. In particular, the audit team shall be able to audit the planning, the performance and the results of the following activities:

- Reviews of the architecture and of the configuration of a cloud service's system components;
- Reviews of the CSP's source code and related documentation;
- Penetration testing of the controls implemented to satisfy the audit criteria, including the EUCS service requirements.

In particular, during every conformity assessment, the audit team shall have the ability to audit the work performed by the CSP and by testing laboratories on vulnerability identification, and to audit the multi-year work program describing the work items to be performed in the following years and audited in future conformity assessments.

In addition to core competencies, this implies that the audit team shall also regularly update their knowledge about the general threat landscape, about the specific threat landscape for cloud services, and more specifically about the threats faced by the specific categories of cloud services implemented by their customers.

E.3 ADDITIONAL REQUIREMENTS FOR LEVEL CS-EL4

For CABs that issue certificates or perform audit activities at evaluation level CS-EL4, additional requirements shall be fulfilled, mostly related to the assessment of the EUCS service requirements around the independence from non-EU laws (as defined in Annex J:Annex J., Protection of European data against unlawful access). These requirements are mostly legal and financial and related to audit activities of specific requirements, in particular relative to the control of the CSP. The conformance of CABs to these requirements will be verified during the authorization process performed by the NCCA before notifying a CAB to the European Commission.

These requirements mostly apply to the audit team, which means that the competences need to be available in the team, but not by every member of the team. A single auditor or technical expert may be sufficient.

The competences are strongly related to the requirements defined in the Annex J: on Protection of European data against unlawful access for evaluation level CS-EL4. In particular, the audit team shall be able to audit the planning, the performance and the results of the following requirements:

- Risk assessment related to extra-territorial application of non-EU laws;
- Absence of effective control from non-EU entities;
- Presence of headquarters in the EU.

In addition to core competencies, this implies that the audit team shall also regularly update their knowledge about the general legal landscape, about the specific legal landscape for cloud services, and more specifically about the legal threats faced by the specific categories of cloud services implemented by their customers.

E.4 SPECIFIC REQUIREMENTS FOR TESTING LABS FOR LEVELS CS-EL3 AND CS-EL4

At evaluation levels CS-EL3 and CS-EL4, the conformity assessment needs to include specific testing activities related to vulnerability identification, and there is an obligation to have some of these testing activities performed by an accredited and authorized CAB.

The CABs performing these testing activities shall be accredited to ISO/IEC 17025, which is the harmonized standard for testing laboratories, which applies to the testing of cloud services. For this accreditation, the ISO/IEC 17065 requirements will be complemented by additional requirements specific to the EUCS, to be defined in a separate document, which will be provided as guidance by ENISA with the support of the ECCG, as a Technical Specification or International Standard by CEN-CENELEC, or as a combination of both.

These documents shall define competence requirements for the various roles in the performance of testing activities, and they shall include specific requirements related to the testing of cloud services.

These requirements mostly apply to the testing team, which means that the competences need to be available in the team, but not by every member of the team. A single tester, auditor or technical expert may be sufficient.

Since testing laboratories perform conformity assessment activities for evaluation levels CS-EL3 and CS-EL4, they shall be authorised by their NCCA. Detailed authorisation requirements should be included in guidance provided by ENISA with the support of the ECCG, but the high-level requirements are defined below.

The competences are strongly related to the technical requirements defined in the section on vulnerability identification and penetration testing for evaluation levels CS-EL3 and CS-EL4. In particular, the testing team shall be able to plan, execute and analyse the results of the following activities:

- Reviews of the architecture and of the configuration of a cloud service's system components;
- Reviews of the CSP's source code and related documentation;
- Penetration testing of the controls implemented to satisfy the audit criteria, including the EUCS service requirements.

Testing laboratories shall also have plans to maintain the competence of their teams, to ensure that they follow the evolution of cloud computing technology and of attack techniques that may apply to cloud computing and to other controls typically implemented by CSPs.

The following set of skills, inspired from [PASSI], should be considered for inclusion in the required skills for testing labs as requirements for the audit team (i.e., at least one auditor needs to master each required skill):

- networks and protocols:

- network protocols and infrastructures;
- common application protocols and infrastructure service;
- configuring and securing of the main network components on the market;
- security equipment and software:
 - access control solutions, including firewalls, zero-trust architecture
 - storage and backup systems, including shared storage
 - cryptography devices, including communications encryption devices and hardware security modules;
 - authentication servers;
 - reverse proxy servers;
 - logging management solution;
 - penetration detection and prevention equipment;
 - client-side security software
- operating systems (environment and hardening):
 - major operating systems, at least UNIX/Linux and Microsoft);
 - embedded operating systems, if relevant;
 - virtualisation solutions;
 - containerisation solutions.
- cloud computing:
 - cloud computing security principles;
 - architecture of major infrastructure cloud services;
 - identity and access management in cloud computing;
 - security monitoring, alerting and audit trail, incident detection and response in cloud computing;
 - devops security;
- application layer:
 - security development guides and principles;
 - application architectures (client/server, n-tier, etc.);
 - languages used for programming or configuring devices and systems;
 - cryptographic mechanisms;
 - application base (web and application servers, DBMS, software packages)
- attacks:
 - principles and methods of application penetration;
 - bypassing of software security measures;
 - vulnerability exploitation and privilege escalation techniques;

In addition to the accreditation's requirements, the proficiency of the audit team regarding the skills listed above and included in accreditation requirements shall be considered as an additional competence requirement to be tested by the NCCA in the context of the authorisation process.

The NAB and NCCA should consider to optimise the process by combining the accreditation and authorisation processes for testing labs.

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 8, Evaluation Methods and Criteria, and Chapter 17, Certificate Format

POLITICO

F.1 INTRODUCTION

The objective of this Annex is to define requirements and 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, in particular for cases when an EUCS conformity assessment is performed jointly with another kind of assessment (ISO-based, ISAE-based, or EBCA).

F.1.1 Conventions used in this annex

Every section below starts with an introduction, including an overview of a document type, 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>, which is used for cross-referencing items.

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 and execution phase
 - i) The Preliminary Activities Planning document, to be prepared by the CAB at the beginning of the conformity assessment and updated with the results during the planning phase of the audit.
 - ii) The Detailed Audit Plan and Execution, to be prepared by the CAB before the audit and updated with the results all along the audit.
- For the reporting phase
 - i) The Evaluation Report, to be prepared by the CAB to
 - (1) report on the audit of the cloud service from the CSP;
 - (2) report on the assurance provided by the CSP's subservice providers and to conclude on the evaluation by providing a certification recommendation.
 - ii) The Review report, to be prepared by the CAB after the review of the Evaluation Report.
- For the certification phase
 - i) The Certification Report, to be prepared by the CAB when the certificate is issued

These documents do not all have the same usage and availability:

- The Application Document and Evaluation Report are shared between the CSP and the CAB.

- The CSP shall make the Evaluation Report available to the CABs of its customers applying for certification based on composition with their cloud service.
- The CSP shall make the Evaluation Report available to its customers upon request, possibly sharing a version specifically prepared by the CAB that issued the certificate by replacing sensitive sensitive information by clearly identified placeholders that explain why the information was removed.
- 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 CABs to their NCCA and NAB for review or assessment.

Finally, the Evaluation Report is only available in a version suitable for the CS-EL2 and above evaluation levels. A version suitable for the CS-EL1 assurance level will be provided in a later phase, together with the questionnaire.

POLITICO

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 the preparation for an application for a conformity assessment related to the certification of a cloud service. The document shall include the information that a CAB needs to start a conformity assessment. The application document provides evidence of an internal audit executed by the CSP prior to engaging with the CAB.

Title of the document: "Application for the certification of <cloud service> of <name of the CSP>

Mandatory field in the template	Clarification
Section 1: "Identification" This section identifies the cloud service for which the application is submitted.	
CSP Identity	Identity of the CSP requesting the conformity assessment
CSP Contact	Identification and contact details for the lead contact at the CSP that will support the conformity assessment process
Service Name	Commercial name of the CSP's cloud service for which the conformity assessment is requested
Short Description	A short description of the functionality of 'Service Name'
Evaluation Level	The evaluation level for which the conformity assessment is requested. Valid values are CS-EL1, CS-EL2, CS-EL3 and CS-EL4
Extension Profiles	The list of extension profiles applicable to the cloud service
Application Type	Type of conformity assessment requested by the CSP. Valid values are 'initial', 'surveillance', 'recertification' or 'special'.
Application Period	When applicable, the period to be considered by the CAB for the assessment of operational effectiveness.
Section 2: "CSP's Management Statement" This section is the CSP's management statement that the description accurately and fairly describes the cloud service and the applicable controls as designed, implemented by the CSP and, if applicable, is operating effectively.	
Statement	This is a written statement by the top management of the CSP confirming that the description accurately and fairly describes the cloud service and the applicable controls as designed, implemented by the CSP and, if applicable, operating effectively.
Section 3: "CSP's Description of its cloud service" This section is the CSP's assessment of the cloud service's implementation of the EUCS requirements.	
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, datacentres, servers, other hardware.
- Software	The programs and system software that supports the 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).

Mandatory field in the template	Clarification
3.3: Service Boundaries	The boundaries of the system subject to certification
3.4: Subservices	The subservices that are significant to the operation of the cloud service
3.6: Information for customers	Reference to the EUCS control requirements framework
- Supplementary information	List of the supplementary cybersecurity information to be made publicly available by the CSP
- Transparency information	Information to be made transparent to fulfil the EUCS requirements
- Complementary User Entity Controls, CUEC	List the applicable CUECs (controls to be applied by CSCs)
- Mapping of contractual clauses to certification requirements	Points to the contractual clauses for every certification requirement that is tied to such clauses.
3.7: Other information	Additional information the CSP considers relevant to the evaluation of the fulfilment of the EUCS requirements
Section 4: "CSP's description of its control framework" This section is the CSP's description of the implemented controls, and of their mapping to the EUCS objectives and requirements.	
Control objectives	The security objectives and CSPs description of controls
Section 5: "CSP's summary of changes and their impact" This section is only applicable to maintenance assessments (where the value of 'Application Type' is not 'initial'), and it contains the CSP's summary of the changes, together with the CSP's assessment of their impact on the certification of the cloud service .	
Summary of changes	A summary of the changes in the cloud service and in the CSP's control framework, with pointers to the other sections of the document.
Impact analysis	An analysis of the impact of the changes summarized above.
Nonconformities to be addressed	Specifically for 'special' maintenance assessment, the list of the nonconformities that need to be addressed.

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 headquarters 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.

The description shall also include all the elements required in order to fulfill the requirements of the EUCS, including any optional feature, support level or similar condition.

The objective is here to ensure that customers get accurate and easily accessible information about the certified cloud service and the conditions under which the requirements of the scheme are met.

<EVALUATION LEVEL>

This shall define the evaluation level for which the CSP applies for certification; its value shall be one of 'CS-EL1', 'CS-EL2', 'CS-EL3' or 'CS-EL4'.

For the appropriate choice refer to the description of the evaluation levels.

<EXTENSION PROFILES>

This shall be the list of the extension profiles applicable to the cloud service, including for every extension profile its full name, reference number, version number and date of certification.

Extension profiles define additional requirements that are specific to an industry, regulation or use case. The reference list of valid extension profiles is maintained by ENISA.

<APPLICATION TYPE>

This shall define the type of conformity assessment to be performed; its value shall be one of 'initial', 'surveillance', 're-certification' or 'special'.

For Application Types 'surveillance', 're-certification' and 'special', additional information is required in the description of the service.

<APPLICATION PERIOD>

When applicable (evaluation levels CS-EL2, CS-EL3 and CS-EL4), 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 evaluation level.

F.2.2 CSP's Management Statement

<MANAGEMENT STATEMENT>

This is a written statement by the top management of the CSP confirming that the description accurately and fairly describes the cloud service and the applicable controls as designed, implemented by the CSP and, if applicable, as operated effectively. The statement shall be dated and signed, and it shall at least point out that:

- the description filed for certification is complete;
- this description is accurate and up-to-date;
- this description meets the requirements for certification in the EUCS scheme; and
- this description is a true reflection of the processes, procedures and systems in place within the organisation in scope of the certification, including the subservices and organizations involved and the corresponding carve-outs;
- the organisation and its management are committed to comply with all their obligations during the conformity assessment and after certification during the entire life cycle of their cloud service's certificate;
- the management of the CSP declares to be responsible for the abovementioned points;
- the management of the CSP declares to fully cooperate and be transparent to the extent needed to handle the complaints in the procedure for complaints ex Article 63 of the EUCSA;
- the management of the CSP declares that it is providing full cooperation in investigative activities of the NCCA ex Article 58(8) of the EUCSA;
- the management of the CSP declares that it is authorising and approving to cooperate in compliance audits of the certificate issuing body and applicable peer reviews ex Article 59 of the EUCSA, and if applying for evaluation levels CS-EL3 and CS-EL4 to peer assessments as defined in the EUCS ex Art 54(1)(u) of the EUCSA;
- if applying for evaluation levels CS-EL3 and CS-EL4, the management of the CSP declares that all the information provided as evidence relative to the requirements of category PUA, and in particular in the risk assessment relative to non-EU laws or on the effective control of the CSP are complete, accurate and up-to-date.

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. No specific taxonomy is defined in the scheme, but guidance or recommendations about usage of a specific taxonomy may be provided at a later stage.

F.2.3.2 The components of the system

<SERVICE COMPONENTS>

There is no mandatory text for the item <SERVICE COMPONENTS>. This item is the identifier for the information in the items of this paragraph.

<PHYSICAL INFRASTRUCTURE>

This item shall list the physical components that are relevant to the provision of 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 shall list the relevant software application programs and system software underlying the cloud service.

Examples of Software are operating systems, middleware, and utilities.

<PEOPLE>

This item shall list 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 shall list the policies and the automated and manual procedures relevant to the CSP's operation of the cloud service and the fulfilment of the EUCS requirements.

<DATA>

Where applicable, this item shall list 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>

This item shall describe the boundaries of the system under certification.

The description of the boundaries shall also include all the contractual elements required in order to meet the requirements of the EUCS, including any optional feature, support level or similar condition.

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. The objective of the second statement is to ensure that customers get accurate information about the conditions under which the requirements of the scheme are met.

F.2.3.4 Subservices

<SUBSERVICES>

The item <SUBSERVICES> lists all the subservices that are significant to the operation of the cloud service. For each subservice the CSP shall provide:

- the role of the subservice;
- the name of the subservice provider;
- the type and scope of functions and services provided;
- how the EUCS requirements apply to that subservice and to the subservice provider that provides it;
- the complementary subservice organization controls (CSOCs) applicable to the subservice and to the subservice provider that provides it;
- assurance the CSP adheres to the subservice provider's requirements for the secure operation of their service (CUECs);
- assurance the subservice adheres to relevant controls of the EUCS and to the CSOCs defined by the CSP;
- assurance on the CSP assuming responsibility over adherence of the subservice and implementing controls to that avail;
- other assurance information like certificate documentation and ISAE or SOC2 reports

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 format for this information is not defined here, but recommended formats will be defined in guidance to be developed by ENISA with the support of the ECCG.

<SUPPLEMENTARY INFORMATION>

This item shall include a list of the supplementary cybersecurity information to be made publicly available by the CSP in application of Article 55 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 publicly available from 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 CSC 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 cloud service; and
- Any other information listed in the EUCS documentation requirements related to transparency that are relevant to the targeted evaluation level.

The information provided shall be compliant to all the documentation requirements on controls that are relevant to the targeted evaluation level.

Further information about the format recommended for this information will be provided in guidance to be developed by ENISA with the support of the ECCG.

<COMPLEMENTARY CUSTOMER CONTROLS, CUEC>

This item shall list all relevant Complementary User Entity Controls (CUECs) considered in the design of the CSP's cloud service, and those CUECs that are relevant to a CSC's operation of the cloud service in accordance with the EUCS service requirements.

<MAPPING OF CONTRACTUAL CLAUSES TO CERTIFICATION REQUIREMENTS>

This item shall list the contractual clauses that are relevant to the certification, and map each one to the requirement(s) that makes use of the contractual clause, and it shall also include an accessible overview of these contractual clauses.

It may occur that contractual clauses are not fixed, in which case the CSP will have to describe all available options. ENISA may develop a list of the requirements for which such contractual clauses need to be provided.

F.2.3.6 Other

<OTHER INFORMATION>

This optional item may be used by the CSP to provide other information that the CSP considers relevant in context of the certification of its cloud service.

F.2.4 The CSP's description of its control framework

<CONTROL OBJECTIVES>

The item <CONTROL OBJECTIVES> shall define how the security controls defined and implemented by CSP meet the service requirements defined in the EUCS and applicable extension profiles, and if applicable, the relevant requirements on CUECs defined by the CSP's subservice providers. For each such requirement, the information shall include:

- If the requirement is not applicable to the cloud service, an indication of this non-applicability, together with a rationale.
- Otherwise, a list of the CSP's controls, together with a description:
 - controls that contribute to the fulfilment of the requirement;
 - Complementary Subservice Organization Controls (CSOCs); and
 - Complementary User Entity Controls (CUECs)

The content of the <CONTROL OBJECTIVES> shall be organized in a table following the template shown below:

Security Control Objectives and audit criteria	<CSP>'s Description of Controls, assumed CSOCs and CUECs, or Rationale if Security Requirement is not applicable
Security Control Objective: [...].	
ID – Title of Requirement [Description of the Requirement]	ID – Title of Control 1 to meet the Requirement or Rationale if Requirement is not applicable [Control Description/Rationale]
	ID – Title of Control 2 to meet the Requirement [Control Description]
	CSOCs: [CSOC Description] / none CUECs: [CUEC Description] / none

F.2.4.1 CSP's summary of changes and their impact

<CSP'S SUMMARY OF CHANGES AND THEIR IMPACT>

The section is required for surveillance, re-certification and special conformity assessments. 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.

<SUMMARY OF CHANGES>

This item shall list all the changes in the definition and operation of the cloud service and of its supporting organisation since the last conformity assessment performed on the cloud service for this scheme.

The list may reference the controls listed in the following section.

<IMPACT ANALYSIS>

This item shall list all the EUCS service requirements, requirements from extension profiles and relevant requirements on CUECs from subservice providers that may be affected by the changes listed in <SUMMARY OF CHANGES>.

The information provided in this list, together with the description in <SUMMARY OF CHANGES>, 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 'special' 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 nonconformity has been identified;
- The severity of the nonconformity ('minor' or 'major');
- A short description of the nonconformity.

This is strongly related to the <SUMMARY OF CHANGES > and <IMPACT ANALYSIS>, since the requirements listed here should also appear in the <IMPACT ANALYSIS> to indicate that the <SUMMARY OF CHANGES> have addressed the issues.

POLITICO

F.3 AUDIT PLANNING

F.3.1 Preliminary activities planning

PRESENTATION

The paragraph 'Content of the document' in this section defines the recommendations for the "Preliminary activities planning and execution" document.

This document is internal to the CAB. It may be part of the documentation provided by the audit team in addition to the evaluation report as input for the review phase. The CAB is free to modify the format, but the elements of information described below should be included.

A CAB should apply these recommendations in its description of each of the audit activities as defined in Annex C to be performed as a preparation to the detailed audit planning, and in its reporting of these activities.

Mandatory field in the template	Clarification
Section 1: "Audit team" This section describes the preliminary activities of the audit. The items described below shall be filled out for every preliminary audit activity relevant for the targeted evaluation level.	
Audit team leader	Affiliation, contact information and qualification of the audit team leader
Audit team	Affiliation, contact information and qualification of the audit team members
Section 2: "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	Identification of the auditor

CONTENT OF THE DOCUMENT

F.3.1.1 Audit team

The items below are recommended for the description of the personnel assigned to the audit activities.

< AUDIT TEAM LEADER >

The CAB should provide the affiliation, contact information and qualification of the audit team leader.

< AUDIT TEAM >

The CAB should provide the affiliation, contact information, role and qualification of every member of the audit team.

F.3.1.2 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 describe the objective of the activity, as listed in the audit 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) and/or document the people inquired.

<EVIDENCE GAINED>

The CAB should describe the evidence gained from the audit activity.

<CONCLUSION REACHED>

The CAB should describe the conclusion reached for the audit activity.

<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 be identified in the document in a way that unambiguously identifies the member within the audit team.

This identification would typically be the initials of the audit team member, or a signature in the case of a paper document.

F.3.2 Detailed audit plan and execution

PRESENTATION

The paragraph 'Content of the document' in this section defines recommendations for the "Detailed audit plan and execution" document for any audit performed at evaluation levels CS-EL2, CS-EL3 and CS-EL4.

This document is internal to the CAB. It may be part of the documentation provided by the audit team in addition to the evaluation report as input for the review phase. The CAB is free to modify the format, but the elements of information are important to document adequately the audit activities performed, the evidence gained, and the conclusion reached.

A CAB should apply these recommendations in two phases:

- during the definition 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 each control as described by the CSP in its description and relevant for the targeted assurance level.	
CSP's controls reference	The security <u>objective</u> and reference to the <u>CSPs control framework</u> (based on the mapping to the EUCS <u>requirements</u>)
1.1 Audit Procedures	Description of <u>audit activities</u> to be performed
Audit Procedure re Design	
- Nature	Nature of the <u>activity</u>
- Timing	Timing of the <u>activity</u>
- Extent	Extent of the <u>activity</u>
Audit Procedure re Existence/Implementation	
- Nature	Nature of the <u>activity</u>
- Timing	Timing of the <u>activity</u>
- Extent	Extent of the <u>activity</u>
Audit Procedure re Operating Effectiveness	
- Nature	Nature of the <u>activity</u>
- Timing	Timing of the <u>activity</u>
- Extent	Extent of the <u>activity</u> , including sampling
1.2 Execution of audit program	
Sources	Information used and people inquired in support of the <u>activity</u>
Evidence gained	Description of the <u>evidence</u>
Conclusion reached	Conclusion for the <u>activity</u>
Date	Date of the conclusion
Name and Initials	Sign-off by the preparer/executer of the <u>audit activity</u>

CONTENT OF THE DOCUMENT

F.3.2.1 *Characteristics of an audit activity*

The document consists of descriptions of audit activities to be performed to audit how the cloud service fulfils the EUCS requirements. The CAB should describe each audit activity 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.

<CSP'S CONTROL REFERENCE>

The CAB should include the reference to the CSP's control framework and the related audit criteria.

<AUDIT PROCEDURE RE DESIGN >

The CAB should describe the procedure to be executed for auditing the design 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 OF IMPLEMENTATION>

The CAB should describe the procedure to be executed for auditing the existence of an implementation of the control to fulfil the objective and associated requirements, as a list of audit activities, each defined by its nature, timing and extent.

<AUDIT PROCEDURE RE OPERATING EFFECTIVENESS>

The CAB should describe 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 of Audit Procedures*

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 audit criteria.

<SOURCES>

The CAB should describe the information used and people inquired to gain appropriate and sufficient objective evidence.

<EVIDENCE GAINED>

The CAB should describe the evidence that has been gained in the activities related to the audit criteria.

<CONCLUSION REACHED>

The CAB should describe the conclusion reached regarding the design, the existence and the operating effectiveness of the controls under audit.

<DATE>

Date of the conclusion.

<INITIALS>

Sign-off by the preparer/executer of the audit procedures.

POLITICO

F.4 EVALUATION REPORT

The evaluation report is the result of the evaluation phase, and it contains two main parts:

- The report resulting from the audit of the cloud service;
- The report that contains the dependency analysis (if required), together with the final recommendation from the evaluation;

F.4.1 Audit results

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the first part of the "Evaluation report" document, describing the results of the audit.

The first part of the evaluation report is the report from the audit. This 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 EUCS. It 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 <u>CAB</u> in charge of the <u>certification</u>
CAB contact	Identification and contact details for the lead contact at the <u>CAB</u> that will manage the <u>evaluation process</u>
Accreditation details	Details about the ability of the <u>CAB</u> to perform an <u>audit</u> , including <u>authorisation</u> if required
Audit team leader	Affiliation, contact information and qualification of the audit team leader
1.3 CSP	
CSP identity	Identity of the <u>CSP</u> requesting the <u>evaluation</u> .
CSP contact	Identification and contact details for the lead contact at the <u>CSP</u> that supported the <u>evaluation process</u>
1.4 Cloud service	Short summary of the <u>cloud service</u>
Service Name	Commercial name of the <u>CSP's cloud service</u> for which the <u>evaluation</u> is requested
Short Description	A short description of the functionality of 'Service Name'.
Evaluation Level	The evaluation level for which the <u>evaluation</u> is requested. Valid values are CS-EL1, CS-EL2, CS-EL3 and CS-EL4
Extension Profiles	The list of <u>extension profiles</u> applicable to the <u>cloud service</u>
Application Type	Type of <u>evaluation</u> requested by the <u>CSP</u> . Valid values are 'initial', 'surveillance', 'recertification' or 'special'.
Application Period	When applicable, the period to be considered by the <u>CAB</u> for the assessment of <u>operational effectiveness</u> .
Application Number	The registration number assigned to the <u>application document</u> upon receipt by the <u>CAB</u>

Mandatory field in the template	Clarification
Section 2: "CSP's Management Statement" This section is the CSP's management asserts or claims that the description accurately and fairly describes the Cloud Service and the applicable controls as designed, implemented by the CSP and, if applicable, is operating effectively.	
Copied 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 EUCS requirements and control framework.	
Description	From the application document
Internal audit results	Internal audit of the conformity of the cloud service to EUCS requirements (CS-EL1 evaluation 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	An overview of the audit activities and results to be included in the Certification Report
4.2 Audit activities and results	
Reasonable assurance	Description and results of the audit activities (version for the CS-EL2 and CS-EL3 and CS-EL4 evaluation levels)
Limited assurance	Description and results of the audit activities (version for the CS-EL1 evaluation 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 including supporting evidence (if any)
Severity	The severity of the nonconformity , which may be 'minor' or 'major'
Suitability of mitigation	The analysis of the mitigation proposed by the CSP and the CAB's conclusion on that
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 with reasonable assurance that the cloud service is in conformity with the requirements from EUCS, considering the carve-out and the Complementary User Entity Controls .
Disclaimer	A disclaimer indicating that the conclusion needs to be combined with the conclusion of the dependency analysis , to be able to conclude on the issuance of a certificate.

CONTENT OF THE DOCUMENT

F.4.1.1 Identification

Identification of the CAB

<CAB IDENTITY>

With reference to by-laws, the legal identity of the [organisation](#) issuing the report shall be provided, including at least:

- Legal name of the [organisation](#);

- Registration number in Chamber of Commerce or equivalent; and
- Office and headquarter location;

If the organisation operates as a subcontractor for the CAB that will issue the certificate, the same information shall be provided about that CAB.

<CAB CONTACT>

The contact details of the responsible department and of the person that is legally representing the organisation 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 contact details of accreditation body;
- Notification number and contact details of the notifying NCCA and, for evaluation levels CS-EL3 and CS-EL4, if Article 56(6) of the EUCSA 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 audit team lead 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.

<EVALUATION LEVEL>

This item shall include the content of the <EVALUATION LEVEL> item from the Application Document.

<EXTENSION PROFILES>

This item shall include the content of the <EXTENSION 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 management statement*

This section shall contain the content of the <STATEMENT> item 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.

<INTERNAL AUDIT REPORT>

This item is only relevant for evaluation level CS-EL1.

This item shall include the internal audit report 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 EUCS, 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 and, if applicable, to authorisation requirements defined by the EUCS and the NCCA.

<SCOPE>

The scope shall clearly describe the scope of the conformity assessment activities:

- Description of the evaluation activities, with reference to the description
- Reference to the relevant and applicable standards
- Reference to non-applicable requirements
- Description of the carve-out handling, including the handling of CUECs from subservice providers
- Description of the CUECs defined by the CSP for its cloud service

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 key persons inquired.

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 audit results part of the evaluation report shall include disclaimers (inherent limitations) 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 evaluation level at the moment of certification and during the certification life cycle;
- Security controls are evaluated to the best of abilities, required skills and knowledge of the evaluating parties; and
- There is no guarantee that audit and subsequent certification exclude all forms of fraud, misleading or circumvention of controls but the EUCS is aiming to prevent such fraudulent behaviour as much as possible.

F.4.1.5 CAB's audit activities and results

OVERVIEW

<OVERVIEW>

The CAB shall include an overview of the audit activities:

- Overview of the reviewed documentation;
- List of on-site visits;
- Overview of the testing performed; and
- List of (roles of the) key persons inquired.

The overview should be a short summary, without the details provided in the description of the CAB's audit activities. It should also not contain any confidential information, as it is intended to be also included in the publicly available certification report. The lists and overview should not be exhaustive, as long as this is clearly explained, including the selection of key persons inquired.

AUDIT ACTIVITIES AND RESULTS

This section shall contain one of the two subsections listed below, depending on the level of assurance required for the evaluation level targeted by the cloud service.

Limited assurance

This section only applies to evaluation level CS-EL1.

For evaluation level CS-EL1, the main audit activity consists in auditing the results of an internal audit, communicated by the CSP to the CAB as an answer to a questionnaire, together with supporting evidence.

ENISA may collaborate with the ECCG to establish a reference questionnaire with the support of the community, asking specific questions for every applicable requirement, and requiring pointers to evidence in support of the answer. If such a questionnaire has been made available by ENISA, then it shall be used for all CS-EL1 assessments.

Additional questionnaires should be defined for extension profiles defined for the CS-EL1 evaluation level, to complement the EUCS questionnaire.

Such questionnaires shall support at least the following information for every question:

- The reference to at least one service requirement from the EUCS. A requirement may be referred to several times, but all applicable requirements shall be referred to in at least one question.

- A unique identifier of the question.
- The text of the question, corresponding to elements from the requirement.
- The answer from the CSP to the question.
- A reference to evidence supporting the answer. Typically, this would consist of reference to documents provided by the CSP, together with pointer to the relevant content in these documents (e.g., section, page or paragraph number).
- A comment or rationale from the CSP, which could help the CAB understand how the provided evidence supports the answer provided.
- A conclusion from the CAB's analysis indicating conformity, minor nonconformity or major nonconformity.
- A description of the audit activities performed by the CAB.
- An explanation from the CAB of the elements who led them to that conclusion.

The audit activities shall follow the questionnaire and include a review activity for every question. The results shall include the result of the review, as well as, where required the description of complementary activities performed by the CAB, together with their results.

The relevant questionnaires shall be included in the audit results as description of the audit activities and results.

Reasonable assurance

This section only applies to evaluation levels CS-EL2, CS-EL3 and CS-EL4.

The CAB shall provide the following table, which presents the CAB's audit activities 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>
Carve-out	Ref. X	Handled by subservice provider X and covered by ISAE3402 type II report of X

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 service requirements from the EUCS that are not being fulfilled.

Although the audit activities are presented following the CSP's organisation of controls, nonconformities need to be related to a specific objective and service requirement. If a nonconformity is related to multiple controls in the CSP's framework (e.g., if the combination of controls leaves a gap), the CAB should reference a single nonconformity and to provide a single analysis in this section.

<NONCONFORMITY>

This item shall include a description of the nonconformity including supporting evidence (if any).

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) including justification.

<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 and the CAB's conclusion on that.

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 verify the success of the mitigation.

Note that the mitigation of a major nonconformity is considered successful if it leads to conformity or to a minor nonconformity. In the case of a minor nonconformity, it is also listed in the section.

F.4.1.6 CAB's conclusion

This section is the audit conclusion (with limited or reasonable assurance, depending on the targeted evaluation level) that the cloud service as described by the CSP is in conformity with the requirements from the EUCS, considering the carve-out and the CUECs, pending the result of the dependency analysis. It shall be dated and signed by the audit team leader.

Two different versions are provided, corresponding to the different levels of assurance used in the conformity assessments for the different evaluation levels.

Limited assurance

<CONCLUSION>

This item shall contain the audit conclusion of the audit team regarding the results of the audit, in terms of providing limited assurance that the cloud service is in conformity with the requirements from the EUCS taking into account the carve-out and the CUECs, indicating:

- whether or not the description fairly presents the CSP's cloud service that was designed and implemented in accordance with the description and presented in the management assertion; and
- whether or not the controls stated in the description were suitably designed, existed and were implemented to provide limited assurance that the EUCS requirements applicable for the targeted evaluation level would be met,
- if applicable, whether or not the subservice organizations and CSCs applied the complementary controls assumed in the design of CSP's cloud service throughout the specified period.

The conclusion shall clearly indicate the recommendation of the audit team, together with a justification. Since this is limited assurance, a conformity audit conclusion shall be formulated as a negative statement that the audit team did not identify any nonconformity.

Reasonable assurance

<CONCLUSION>

This item shall contain the audit conclusion of the audit team regarding the results of the audit, in terms of providing reasonable assurance that the cloud service is in conformity with the requirements from the EUCS taking into account the carve-out and the CUECs, indicating:

- whether or not the description fairly presents the CSP's cloud service that was designed and implemented in accordance with the description and presented in the management assertion; and
- whether or not the controls stated in the description were suitably designed, existed, were implemented and operated effectively to provide reasonable assurance that the EUCS requirements applicable for the targeted evaluation level would be met,
- if applicable, whether or not the subservice organization(s) and CSCs applied the complementary controls assumed in the design of CSP's cloud service throughout the specified period.

The conclusion shall clearly indicate the recommendation of the audit team, together with a justification. Since this is reasonable assurance, a conformity audit conclusion shall be formulated as a positive statement that the audit team was able to reach a reasonable level of assurance.

<DISCLAIMERS>

To be able to conclude whether or not the cloud service can be certified, this conclusion needs to be combined and with the assurance or other reports (like ISO, ISAE, SOC2) provided by the subservice providers. These reports need to be analysed in the dependency analysis and combined with the audit results to reach a final conclusion.

F.4.2 Dependency analysis and final recommendation

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for second part of the "Evaluation report" document, including the dependency analysis and final recommendations.

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 conditional section identifies the CAB in charge of the certification, the audit team in charge of the dependency analysis, and the cloud service being audited. Same as for the Audit Results.	
Section 2: "CSP's Management Assertion" This conditional section is the CSP's management assertion that accurately and fairly describes the cloud service and the applicable control framework. From the Application document.	
Section 3: "CAB's Responsibility Assertion" This conditional section is the CAB's management assertion about their responsibility. Same as for the Audit Results	
Section 4: "CAB's Dependency Analysis Activities and Results" This section describes the CAB's dependency analysis activities and results.	
5.1 Presentation	An high-level presentation of the audit activities and results, to be included in the Certification Report
5.2 Activities and results	Analysis to be performed on each subservice provider
Reasonable assurance	Description and results of the dependency analysis activities (version for the CS-EL2 and CS-EL3 and CS-EL4 levels)
- Assurance information	Verification of the suitability of the nature of assurance information 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 dependency analysis activities (version for the CS-EL1 evaluation 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
Section 5: "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 audit conclusion for the dependency analysis

Mandatory field in the template	Clarification
Recommendation	Combined <u>audit conclusion</u> for the combination of main <u>audit</u> and <u>dependency analysis</u> and recommendation for the <u>certification decision</u>

CONTENT OF THE DOCUMENT

F.4.2.1 Identification

This section shall have the same content as the one described in the Audit Results section (F.4.1.1).

This section is only required if this second part is presented in a standalone document separate from the audit results.

F.4.2.2 CSP's management assertion

This section shall contain the CSP's management assertion from the Application Document.

This section is only required if this second part is presented in a standalone document separate from the audit results.

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 evaluation level CS-EL1.

This item shall include the results of the internal dependency analysis provided by the CSP following the template provided by the CAB for assessing the adequacy of the assurance information available and the sufficiency of the controls covered by that assurance information.

F.4.2.4 CAB's responsibility assertion

This section has the same content as the one described in the Evaluation report (F.4.1.4).

This section is only required if this second part is presented in a standalone document separate from the audit results.

F.4.2.5 CAB's dependency analysis activities and results

Overview

<OVERVIEW>

The CAB shall include an overview of the dependency analysis activities:

- List of subservice providers, which may be partial (key subservice providers) if explicitly stated.
- List of provided assurance information
- Summary of the CAB's analysis and nonconformities

The overview should be a short summary, without the details provided in the description of the CAB's dependency analysis activities. It should also not contain any confidential information, as it is intended to be also included in the publicly available Certification Report. It is explicitly allowed to list only key subservice providers, as long as the overview mentions that some subservice providers are not listed.

Dependency analysis activities and results

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.

The elements provided are the same for all evaluation levels, but the level of detail expected depends on the targeted evaluation level, and is less detailed for evaluation level CS-EL1.

<ASSURANCE INFORMATION>

This item shall include a description of the nature of the assurance information followed by an analysis of its suitability. The following elements shall be considered:

- Nature of the assurance information documents (ISAE report, certificate, evaluation report, 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 provider's controls.

If the assurance information is an EUCS certificate, then checks are only required of the certificate validity, of the evaluation level and if needed, of the extension profiles.

More information about acceptable reports and certificates and specific attention points for every type of report should be provided as guidance.

<DOCUMENTATION ORIGIN>

This item shall include a description of the organisation who issued the report or certificate, followed by an analysis of its suitability. The following elements shall be considered:

- Identity of the issuing organisation and, if required of the lead auditor;
- Competence of the issuing organisation and lead auditor (accreditation, personal certification);
- Independence of the issuing organisation and lead auditor (accreditation, other indication)

If the assurance information is an EUCS certificate or report, then no checks are required.

<SCOPING>

This item shall include a description of the scope of the assurance information, 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 information 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 information, followed by an analysis of their impact. The following elements shall be considered:

- Nonconformities identified in the assurance information that may affect the CSP;
- Severity or qualification of the nonconformities;
- 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 information available for the subservice provider.

Nonconformities

This section shall list all the nonconformities identified during the audit, including a summary 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 CSOC defined by the CSP.

<NONCONFORMITY>

This item shall include a description of the nonconformity including supporting evidence (if any).

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 information, 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 and the CAB's conclusion on that.

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 verify the success of the mitigation.

Note that the mitigation of a major nonconformity is considered successful if it leads to conformity 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 Evaluation conclusion

This section is the conclusion of the analysis of the evaluation report of the CSP together with the reports and conclusions provided by the subservice providers, about the fulfilment of EUCS requirements by the cloud service, to the extent determined by this overall assessment, which shall be dated and signed by the audit team leader.

<DEPENDENCY CONCLUSION>

This is the conclusion of the audit team regarding the dependency analysis, considering all subservice providers.

<RECOMMENDATION>

This item shall include the final recommendation of the audit team, based on the audit conclusions of the main audit and of the dependency analysis. The audit team shall determine whether or not the cloud service meets the EUCS requirements for the targeted evaluation level and shall provide a recommendation regarding the certification of the cloud service.

The recommendation shall be dated and signed by the audit team leader.

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. No template is provided.

POLITICO

F.6 CERTIFICATE PACKAGE

F.6.1 Certificate

The requirements for the content of certificates are defined in the scheme itself (Chapter 17, Certificate Format). No additional information is required here.

A graphical template may be provided by ENISA in collaboration with the ECCG, which should be followed by CABs if available.

F.6.2 Certification report

PRESENTATION

The paragraph 'Content of the document' in this section defines the requirements for the "Certification 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 Certification Decision Report" This section confirms the evaluation and review work done by the CAB to conclude on issuing the certificate.	
Scope	Description of the <u>scope of certification</u> , from the <u>evaluation report</u>
CSP Management Responsibilities	Description by the <u>CAB</u> of the <u>CSP's</u> management responsibilities in the <u>evaluation</u> , from the <u>evaluation report</u>
CAB responsibilities	Description by the <u>CAB</u> of the <u>CAB's</u> responsibilities in the <u>evaluation</u> and of the inherent limitations of the <u>evaluation</u>
Certification decision	Description by the <u>CAB</u> of the outcome of the <u>evaluation</u> , which led to the positive <u>certification decision</u>
Section 2: "CSP Management Statement" 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 <u>top management</u> of the CSP, identical from the <u>application document</u> and the <u>evaluation report</u>
Section 3: "Cloud service scope" This section is the CSP's assessment of the cloud service's implementation of the EUCS requirements.	
Background	Information on the <u>CSP</u> as an organisation
Cloud service	The <u>cloud service</u> in scope for the <u>evaluation</u> , including the commercial names used for the <u>cloud service</u> .
Service components	A list of the main components of the <u>cloud service</u>
Section 4: "Principle Service Commitments and System Requirements" Description of the cloud service, the CSP commitments and requirements.	
Description	General description provided by the <u>CSP</u> of its approach to cybersecurity assurance and compliance to the EUCS

Mandatory field in the template	Clarification
a) Physical Infrastructure	Description by the CSP of physical structures at the CSP that support the development and operation of the cloud service.
b) People	Description by the CSP of (types of) personnel at the CSP involved in the governance and operation of the cloud service
c) Procedures	Description by the CSP of automated and manual procedures at the CSP involved in the governance and operation of the cloud service
d) Data	Description by the CSP 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 CSC data, and about applicable laws.
Section 6: "Overview of assessment" This section includes the overview of the assessment activities performed by the CAB.	
Audit overview	Overview of the audit activities
Dependency analysis overview	Overview of the dependency analysis activities

CONTENT OF THE DOCUMENT

F.6.2.1 Independent Certification Decision Report

<SCOPE>

This item shall contain a description of the scope of certification, including at least:

- The targeted evaluation level
- If applicable, the list of claimed extension 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 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 certified cloud service meets the EUCS requirements
- An overview of the subservices and how they have been considered to contribute meeting the EUCS 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 organisation 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.

<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 *Additional information*

This section includes information that may be useful for the CSC to improve their understanding of the activities performed in the context of the certification and to provide an elementary level of assurance information about the conformity assessment activities that led to the certification of the cloud service.

<AUDIT OVERVIEW>

If present, this item shall include the content of the <OVERVIEW> section from the audit results section of the evaluation report.

<DEPENDENCY ANALYSIS OVERVIEW>

If present, this item shall include the content of the <OVERVIEW> section from the dependency analysis section of the evaluation report.

POLITICO

ANNEX G: CERTIFICATION LIFE CYCLE AND CONTINUED ASSURANCE

PURPOSE	This annex describes additional content related to the chapters on certification life cycle 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

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 CS-EL2 and above), Annex D: (Assessment for level CS-EL1) 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 Surveillance assessment

A surveillance assessment shall be performed every year during the validity period of the certificate. In a surveillance 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 evaluation levels.

The CAB shall at least:

- Obtain an understanding of the changes operated since the last conformity assessment in the cloud service and the CSP's controls to meet the EUCS security objectives and related service 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 evaluation levels CS-EL2 and above.

The CAB shall at least:

- Select a subset of controls, including at least the controls for which nonconformities have been detected in the previous conformity assessment and the controls defined in a dedicated guidance to be provided on a regular basis through the EUCS maintenance structure.
- Assess the suitability of the design of the selected controls.

Effectiveness assessment

These activities are only required at evaluation levels CS-EL2 and above.

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 conformity assessment and if they have been operating for less than 3 months (6 months for levels CS-EL3 and CS-EL4), the CAB shall assess to which extent of the changes affect their ability to assess the operating effectiveness of the controls.

G.1.2 Re-certification assessment

A re-certification assessment shall be performed in the year before the expiry of a certificate, in order to extend its validity for another 3-year period. Alike an initial assessment, a re-certification assessment of a cloud service shall cover all parts of the conformity assessment methods defined in Annex B: (Meta-approach for the assessment of cloud services), Annex C: (Assessment for levels CS-EL2 and above), Annex D: (Assessment for level CS-EL1) for all EUCS requirements defined in Annex A: (Security Objectives and requirements for Cloud Services).

However, in the context of a re-certification 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 the changes on other controls.

G.1.3 Special assessment

A special assessment shall be performed when a certificate has been suspended, before the suspension is lifted and the certificate fully restored. A special assessment may also be triggered by a CSP at any time, typically after performing significant changes to their cloud service or to their control framework, which require a specific assessment

In a special 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 nonconformities have been detected, or on the changes made by a CSP to their cloud service or to their control framework.

In a special 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 evaluation levels.

The CAB shall at least:

- Obtain an understanding of the changes operated since the last assessment in the cloud service and to the CSP's controls to meet the EUCS security objectives and related service 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 evaluation levels CS-EL2 and above.

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 levels CS-EL3 and CS-EL4), the CAB shall assess to which extent of the changes affect their ability to assess the operating effectiveness of the controls.

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 activity 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, including financial support.

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 EUCS, 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 that 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 together with their analysis to the NCCA.

If the CAB 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 relevant process(es) shall be triggered.

G.2.3 Vulnerability assessments

When they become aware of a vulnerability that may affect a certified cloud service, the CAB shall request a vulnerability assessment from the CSP. This may happen in particular when the NCCA requests the CAB to investigate a vulnerability.

Then, the process should proceed 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 whether or not the vulnerability affects their cloud service, and if it does, an estimate of the severity of the vulnerability, as well as a description of the mitigation plan that they have designed, accompanied by supporting documentation if required;

- The CAB shall then analyse the answer from the CSP, and if applicable, transmit the CSP's answer with their analysis back to the NCCA.

If the CAB 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 relevant process(es) shall be triggered.

G.2.4 CAB audits

If the NCCA that authorized a CAB or the NAB that accredited a CAB have doubts about the conformity of the CAB to their accreditation or authorisation requirements, the relevant authority shall engage with the CAB to perform all necessary verifications, including any conformity assessment activity that is required.

No specific conformity assessment activities are required by the EUCS for such situations, except where it impacts directly the operation of the EUCS:

- If nonconformities are detected and the relevant authority decides to suspend or withdraw the accreditation or authorisation of the CAB, they shall notify the Commission and ENISA of the decision taken and of its consequences and follow-up actions.
- If nonconformities are detected, the relevant authorities shall assess the impact of these nonconformities on the certificates issued or maintained by the CAB, and inform ENISA of any change required in the status of the certificate, such as suspension or withdrawal.

The NCCA and NAB should coordinate their actions when such situations occur.

ANNEX H: EXTENSION PROFILES

PURPOSE	This annex describes the applicable procedure for the management of EUCS extension profiles, throughout their life cycle.
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Section 24.1, Extension Profiles

POLITICO

H.1 INTRODUCTION

H.1.1 Background and presentation

The EUCS is a horizontal certification scheme, which defines a baseline that can be used for any cloud service. In addition, individual sectors or specific cloud architectures might impose additional security requirements that go beyond of what is relevant for a horizontal scheme and what is included in the EUCS. Such additional requirements may, for instance, be imposed by specific EU directives or regulations³³, or by customer demand in certain markets, including to support the CSCs to fulfil the sector-specific regulation.

To maintain the wide horizontal applicability of the EUCS while at the same time recognizing the need for specific requirements, the EUCS supports the definition of Cloud Service Extension Profiles (CSEP), which allow to extend the EUCS service requirements for a given evaluation level and a defined specific context without weakening the assurance provided by the EUCS evaluation levels.

By creating a CSEP, the CSEP developer can strengthen EUCS service requirements ("enhanced service requirements") or add new service requirements corresponding to a given use case.

Before it can be used in the certification of cloud services, a CSEP shall be certified by a CAB, to ensure that it fulfils the requirements defined in this annex. The corresponding certificate, including a link to the CSEP, then needs to be published by ENISA on its certification web site.

Once a CSEP is certified and published, a CSP may claim conformity to that CSEP in their application for the certification of a cloud service. The CAB will then consider the requirements from the CSEP in its certification activities, and deliver a certificate that mentions conformity to the CSEP. A CSP may claim conformity to several CSEPs, and conformity to a CSEP may be a requirement from an EU Cybersecurity Certification Scheme that relies on the EUCS for the certification of a cloud service.

H.1.2 Specific terminology

A **Cloud Service Extension Profile (CSEP)** is a document that describes requirements on cloud services.

In the rest of this annex, the EUCS requirements, as defined in Annex A, will be referred to as the **EUCS requirements**, to distinguish them from the requirements defined in a CSEP, which will be referred to as the extended requirements. Altogether, in the context of a cloud service conformity assessment, the EUCS requirements together with the extended requirements from the CSEPs to which the CSP claims conformity make the certification requirements (part of the audit criteria).

The entity developing a CSEP is the CSEP developer, and remains in charge of the CSEP throughout its life cycle.

H.2 LIFE CYCLE OF EUCS EXTENSION PROFILES

The life cycle of a CSEP includes the following phases:

- Development
- Certification
- Publication
- Withdrawal

Once a CSEP has been certified and published, minor corrections and updates may be performed (including a special assessment), but there is no specific procedure for the revision of a CSEP with more significant updates, so the

³³ e.g. European Electronic Communications Code (EECC) Directive, 2018 - technology neutral

process is to develop a new CSEP and to withdraw the previous one (not necessarily at the same time, in order to guarantee a smooth transition from one version to the next).

H.2.1 Development of extension profiles

A CSEP developer shall be a legal entity established in the EU. Examples of CSEP developers include:

- Individual companies (e.g., CSPs), who want to build a CSEP as a response to a specific issue;
- Associations or industry groups who want to build a CSEP that can be useful for their members (either as CSPs or as CSCs);
- Standard defining organisations;
- ENISA, in the context of the development of a new European cybersecurity certification scheme, requiring the definition of specific criteria for cloud services;

CSEPs may also be developed in relation to an EU regulation or directive, to impose specific security measures on a specific category of CSPs, for instance belonging to a specific industry.

The CSEP developer shall be responsible for the CSEP throughout its life cycle. The CSEP developer shall support the costs associated to the creation and validation of the CSEP, and any complaints or issues related to the CSEP shall be addressed to the CSEP developer.

The CSEP developer shall write the CSEP using the principles used in the EUCS, for the definition and formatting of service requirements, as defined in the first sections of Annex A: (Security Objectives and requirements for Cloud Services) and also for the terminology that is defined in Annex K:. In addition, the CSEP developer should consider the following documents:

- the ISO/IEC 17007:2009 – Guidance for drafting normative documents suitable for use for conformity assessment;
- ISO/IEC Directives, Part 2 – Principles and rules for the structure and drafting of ISO and IEC documents.

A CSEP developer shall use as a basis the latest available version of the EUCS. When a new revision of the EUCS is adopted, then new CSEPs need to refer to that new version, and CSEPs referring to older revisions of the EUCS shall be withdrawn before the end of the new EUCS release's adoption period.

H.2.2 Certification of extension profiles

In addition to cloud services, it shall be possible in the EUCS to certify CSEPs, to ensure that the CSEPs satisfy the requirements defined below, and in particular that they define extended requirements that are actionable and auditable, and that do no conflict with EUCS requirements.

The certification of a CSEP shall be performed by a CAB that has been notified to certify cloud services at least at evaluation level CS-EL2 and at the evaluation level targeted by the CSEP. It consists of an audit of the CSEP by the CAB to achieve reasonable assurance that the CSEP satisfies all the requirements defined in EUCS for CSEPs.

The CSEP shall contain all required information and evidence to perform its evaluation, including rationales describing how, from the point of view of the CSEP developer, the CSEP meets the requirements of EUCS for CSEPs.

H.2.3 Publication of extension profiles

ENISA shall maintain a list of published CSEPs. CABs shall notify ENISA upon certification of a CSEP, and ENISA shall then list the certificate of the CSEP on its Web site with the "published" status.

NOTE: The publication of a CSEP by ENISA on the Certification Web site does not by itself constitute an endorsement or recognition of the CSEP by ENISA. It simply indicates that the CSEP has been certified by a notified CAB. Endorsement or recognition of a CSEP will have to come from the community for which the CSEP is developed³⁴.

H.2.4 Withdrawal of extension profiles

When a CSEP becomes obsolete, the CSEP developer shall notify ENISA that the CSEP needs to be withdrawn, and ENISA shall then modify the status of the CSEP from “published” to “withdrawn”.

At the end of the adoption period of an EUCS release, all CSEPs based on previous versions of the EUCS become obsolete, and ENISA shall then modify the status of these CSEPs from “published” to “withdrawn”.

Withdrawn CSEPs shall remain accessible from ENISA’s certification web site for at least five (5) years after the withdrawal of the CSEP.

H.3 REQUIREMENTS ON EUCS EXTENSION PROFILES

The requirements on CSEPs are independent of the targeted evaluation level. A CSEP shall include requirements that are adapted to the targeted evaluation level, but the CSEP itself is evaluated independently of this targeted evaluation level.

H.3.1 EP-01 Structure and content

H.3.1.1 Objective

Documents defining a CSEP follow a common structure and include the expected content.

H.3.1.2 Requirements

<p>The CSEP developer shall use the following structure for the description of a CSEP:</p> <ul style="list-style-type: none"> • Introduction, providing a description of the CSEP and its intended use; • Conformance claims, stating the CSEP’s claims of conformance to a specific version of the EUCS, to the targeted EUCS evaluation level and if required, to other CSEPs. • Scope, defining the targeted cloud services and their intended use, industry requirements, regulation and/or the specific technological or business contexts to which the CSEP applies; • Security problem, identifying the motivation for the CSEP from a security viewpoint, including at least a definition of specific assets, threats, and security objectives; • Service requirements, documenting the additional requirements defined in the CSEP following the structure used in Annex A. 	EP-01.1
<p>The CSEP developer shall include in the CSEP rationales justifying how the various elements of the CSEP’s structure are adequate and properly related to each other, and in particular:</p> <ul style="list-style-type: none"> • How the security story matches the description, conformance claims and scope of the CSEP; • How the extended requirements match the security story; • How the CSEP components satisfy the present requirements. 	EP-01.2
<p>The CSEP developer shall only define CSEPs of EU-wide applicability.</p>	EP-01.3

H.3.1.3 Additional information

- Requirement EP-01.3 is intended to enforce that CSEPs are not used to introduce National schemes within the scope of the EUCS.
- ENISA, in collaboration with the ECCG, may provide additional guidance related to requirement EP-01.1, in particular a detailed template for CSEP documents.

³⁴ In some cases, for instance if a CSEP is developed as part of another European cybersecurity certification scheme, ENISA may contribute to this recognition, but not as part of their work on the development and maintenance of EUCS.

H.3.2 EP-02 CSEP requirements

H.3.2.1 Objective

The requirements defined in a CSEP follow principles about their consistency with EUCS.

H.3.2.2 Requirements

The CSEP developer shall not include in a CSEP any requirement that contradicts any certification requirement defined in EUCS or that weakens any <u>certification requirement</u> defined in EUCS that applies at the targeted evaluation level.	EP-02.1
The CSEP developer shall only include in the <u>CSEP requirements</u> that are consistent with the definition of the targeted EUCS evaluation level and with the <u>requirements</u> already defined for that <u>evaluation level</u> .	EP-02.2
The CSEP developer shall include in a <u>CSEP requirements</u> that are both necessary to address the security objectives stated in the <u>CSEP</u> and sufficient to meet these <u>objectives</u> .	EP-02.3
<p>The CSEP developer shall minimize the changes in the definition of requirements in a CSEP:</p> <ul style="list-style-type: none"> • If a <u>requirement</u> is a refinement of an existing EUCS requirement, the CSEP shall define it in the same requirement category and explicitly reference the refined requirement; • If a <u>requirement</u> is new but is associated to an existing category, the CSEP shall define the requirement in that category and explain how it complements the other <u>requirements</u> in this category; • If a requirement does not belong to an existing category, the CSEP shall define a new category for the requirement, including an <u>objective</u>, and explain how it differs from the other categories and how it relates to them. 	EP-02.4
<p>The CSEP developer shall ensure that all new <u>requirements</u> are actionable and auditable by abiding to the following principles:</p> <ul style="list-style-type: none"> • Inclusiveness, where the extended requirements defined in a CSEP shall be inclusive and incremental compared to the EUCS requirements; • Clarity, where the extended requirements defined in a CSEP shall be clearly defined as to confuse neither the CSP implementing a cloud service conformant to the requirement nor the CAB tasked to verify the conformity of a cloud service to the requirement; • Effectiveness, where conformance to the service requirement should guarantee a baseline security level in different cloud services; • Auditability, where the conformity assessment to a requirement shall be possible using the <u>evaluation methods</u> defined in the EUCS. 	EP-02.5

H.3.2.3 Additional information

- An extended requirement defined in a CSEP cannot contradict any EUCS requirement, independently of the evaluation level, because compliance to a CSEP may be claimed in a certificate obtained at a higher evaluation level (e.g., a CS-EL2 CSEP may be referred to in a CS-EL3 and CS-EL4 certificate, so it is important to ensure that this CSEP does not contradict any EUCS requirement defined for evaluation levels CS-EL3 and CS-EL4).
- The mention of certification requirements means that the extended requirements defined in a CSEP shall not contradict the service requirements from the EUCS or from any CSEP to which the CSEP under evaluation claims conformance. However, there is no explicit requirement that requirements in different CSEPs should not contradict each other, but this is implicit if the CSEPs are intended to be used together.

H.4 REQUIREMENTS ON THE CERTIFICATION AND PUBLICATION OF EUCS EXTENSION PROFILES

The certification of a CSEP shall be performed following the conformity assessment principles used for the conformity assessment of cloud services at evaluation level CS-EL2, i.e., the CAB shall provide reasonable assurance through the execution of an audit by an independent auditor that the CSEP meets the requirements defined above.

In order to ensure that they have the appropriate knowledge and competence, the certification of a CSEP shall be performed by a CAB that has been notified to certify cloud services in the EUCS at least for evaluation level CS-EL2, and at least for the EUCS evaluation level targeted by the CSEP to be certified.

The principles defined in Annex B: (Meta-approach for the assessment of cloud services) shall be used for the conformity assessment of the CSEP, but the process shall be simplified as follows:

- The audit shall only rely on the CSEP document, which is expected to contain all the information required for the CAB to reach an audit conclusion with reasonable assurance;
- The process shall not use the document templates provided in Annex F: (Scheme Document Content requirements), since these templates are intended for the certification of cloud services.
- The dependency analysis does not need to be performed.
- The requirements to be considered shall only include the EP-01 and EP-02 categories defined above.

In addition, the conditions of the EUCS that would apply to a cloud service certified at evaluation level CS-EL2 shall also apply to CSEPs, with the following exceptions:

- The CSEP may be, as a cloud service, subject to maintenance for updates or corrections, through a special assessment, but surveillance audits shall not apply to CSEPs;
- The CSEP shall not necessitate the application of monitoring activities described under Chapter 11 (Compliance Monitoring);
- The information provided in a certificate of a CSEP shall be a subset of that provided in a certificate of a cloud service;
- Supplementary cybersecurity information as defined by Article 55 of the EUCSA shall not be necessary.

The certificate of a CSEP shall include the following elements:

- a unique identifier established by the issuer of the certificate, following a specification to be defined by ENISA to guarantee the unicity across the EU and across certificate versions;
- information related to the certified CSEP and its developer:
 - i) name of the CSEP;
 - ii) version of the CSEP;
 - iii) name and contact information of the CSEP developer;
- information related to the evaluation and certification of the CSEP:
 - i) name and contact information of the body or authority that issued the certificate;
 - ii) name of the CAB which performed the audit, when different from the abovementioned body or authority;
 - iii) name of the responsible NCCA;
 - iv) reference to this certification scheme and its version;
 - v) reference to the certification report associated with the certificate;
 - vi) evaluation level from this certification scheme (CS-EL1, CS-EL2, CS-EL3 or CS-EL4) targeted by the CSEP;
 - vii) corresponding assurance level from the of the EUCSA ('basic', 'substantial' or 'high');
 - viii) date of issuance and period of validity of the certificate;

Following the registration of the certificate to ENISA for publication on the certification web site, ENISA will provide a unique link for the certificate, possibly associated to a QR-code, that will point to the certificate's page on ENISA's Web site, to be used in all communication about the certificate, possibly in conjunction to the label, when available.

Each certificate shall be signed by the appropriate responsible person of the authority or body and made available to the NCCA and to ENISA with its associated certification report in electronic form and in English language. In case such documents are produced in a language different from English, a courtesy translation shall be provided.

ANNEX I: 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

POLITICO

I.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.

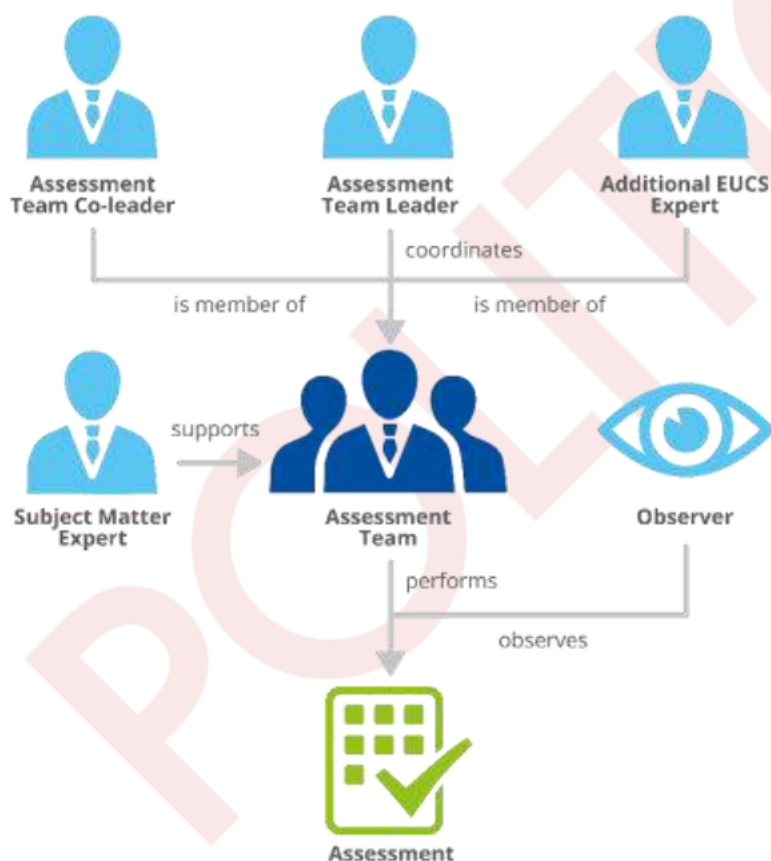
The procedure only defines the process to be followed. In order to be as comprehensive and objective as possible, checklists shall be further developed in cooperation with the ECCG to assist the peer assessment team. These checklists will contain a common understanding of state-of-the-art³⁵ and operating practices.

I.2 OVERVIEW

The primary assessment team shall consist of two EUCS experts (Leader and co-Leader) selected from two CABs issuing certificates at the evaluation levels CS-EL3 and CS-EL4 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 5: 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 evaluation levels CS-EL3 and CS-EL4. In addition, at least one EUCS expert in the assessment team shall have previously participated to the assessment of additional competences of CABs issuing certificates at evaluation levels CS-EL3 and CS-EL4, as listed in Chapter 7 (Specific requirements applicable to a CAB).

³⁵ 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 can 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 audit organisations 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 audit organisations employed or 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.

1.3 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 cloud services for which the CAB has performed a conformity assessment, for review by the peer assessment team. In general, the candidate cloud services shall cover all technical aspects of the audit.

The required number of candidate cloud services is:

- At least two (2) cloud services; and
- At least one (1) cloud service for every audit organisation accredited as subcontractor for the CAB at evaluation levels CS-EL3 and CS-EL4, if applicable.

The requested information and the list of candidate cloud services (and audit organisations) shall be provided by the peer assessed CAB to the peer assessment team within one month after the notification by the ECCG.

The peer assessment team will arrange the dates for the peer assessed CAB and where applicable auditor(s) site visit(s).

1.4 RESPONSIBILITIES OF THE PEER ASSESSED CB

The peer assessed CAB shall provide the following documentation:

- a full description of its scope, organisation and operation, including:
 - the title, address and principal point of contact;
 - its role according to Article 56 of the EUCSA;

- 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 CAB and its internal or external auditors to the protection of audit information and other sensitive information;
- the titles and addresses of the audit organisations 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 EUCS certificates issued by the peer assessed CAB for the last five years;
- two or more EUCS certificates and corresponding 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 persons that perform conformity assessment activities³⁶ for that domain and a description of the evidence used when assessing the competences of these persons.

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 cloud services submitted for consideration need not be entirely complete, there must be records showing that a significant analysis of evaluation and certification activities have been performed, and that the majority of the evaluation report has been delivered to and reviewed by the review and certification team.

In addition to the selected cloud 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 cloud services. This information will be provided to the peer assessment team for their review and selection and shall include:

- a brief overview of the cloud service,
- the type of conformity assessment,
- the status of the conformity assessment (if not completed, then indicate what parts have been completed and what remains to be done),
- the target evaluation level.

³⁶ Including all auditors, as well as personnel involved in review and certification activities.

- any extension 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 audit organisation(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 peer 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 audit organisation(s) visits with the peer assessment team,
- Arranging all necessary approvals to allow the peer assessment team to perform the CAB and audit organisation(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.

I.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 cloud services (and audit organisations) and notification to the peer assessed CAB,
- Drafting the site visit(s) agenda and coordinating it with the CAB,
- 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.

I.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.

1.7 SITE VISIT PHASE

1.7.1 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.

1.7.2 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 necessarily 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 audit organization's technical competence by:

- a visit of the audit organization's site,
- interviews with audit team members on technical items related to the assessment of EUCS requirements.

Findings correspond 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 nonconformity could be either critical or non-critical. A critical nonconformity challenges the reliability of the results established by the assessed CAB. The peer assessment team shall analyse and describe the impact of each critical nonconformity.

At the end of the site visit, the peer assessment team should present the list of findings (at least the draft list of nonconformities 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 nonconformities 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.

1.8 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 nonconformity is provided before issuance of the report, the team can reconsider the criticality of the nonconformity and shall document this change in the report.

The peer assessment team might include into its report relevant results 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 nonconformities 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 from the CAB 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 action 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.

1.9 ADOPTION OF PEER ASSESSMENT REPORT

The following procedure is provided to guarantee adequate involvement of the assessed CAB to demonstrate prompt resolution of nonconformities. 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 peer assessment team is proposed to be adopted as it is;
 - an amended final report from the peer assessment team is proposed to be adopted.

In the case of nonconformities, the opinion to be adopted by the ECCG will include a recommendation to the assessed CAB to resolve such nonconformities 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 nonconformities 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 nonconformities 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 peer assessment team to discuss the status of resolution of the nonconformities. 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 nonconformities) or a fail (residual nonconformities 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.

POLITICO

ANNEX J: PROTECTION OF EUROPEAN DATA AGAINST UNLAWFUL ACCESS

PURPOSE	This annex describes specific requirements to provide some guarantees about the independence from non-EU law
CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE	Chapter 5: Assurance Levels Annex A: Security Objectives and requirements for Cloud Services

POLITICO

J.1 INTRODUCTION

The objective of these specific requirements is to adequately prevent and limit possible interference from states outside of the EU with the operation of certified cloud services. Such interference is possible in many ways, and the following technical measures have been considered to reduce to mitigate this risk:

- The CSC data is stored and processed in the EU by the CSP, including CSC data stored and processed by subservice providers of the CSP.
- The CSC data may only be accessed by the CSP under the control of employees who have undergone a specific screening, and who are located in the EU.
- Any access to a functional component of the CSP's infrastructure by a supplier, typically for support purposes, has to be performed under the control of employees who have undergone a specific screening, and are located in the EU.

In addition, some countries outside of the EU (third countries) have laws with extra-territorial application that may interfere or conflict with Union Law or with the National law of the relevant Member State. In order to mitigate the risk related to the extra-territorial application of such laws, the following technical measures have been considered:

- The contracts for the provision of certified cloud services are governed by the law of a Member State and define only EU courts, tribunals or arbitration bodies to have jurisdiction over disputes related to the contracts.
- Certified cloud services are operated only by companies based in the EU, with no entity from outside the EU having effective control over the CSP.
- CSPs include the risks related to non-EU laws with extra-territorial application in their global risk assessment, and make the information about residual risks available to their customers so they can perform their own risk assessment.

The second set of measures require for their evaluation specific legal and financial competences that are not typically available in CABs, so the related requirement is stated as an eligibility requirement to a certification request, based on an assessment performed by a designated government authority. The role of the CAB shall only be to verify the presence of a positive assessment result issued by the designated government authority.

J.2 SERVICE REQUIREMENTS ON PROTECTION OF EUROPEAN DATA AGAINST UNLAWFUL ACCESS

PLAN THE PROVISION OF A RESILIENT CLOUD SERVICE WHILE MINIMIZING THE RISK OF DEPENDENCE OVER THIRD COUNTRY LEGISLATION.

Term	Definition
high administration privileges	<u>access rights</u> that allow elevation of privilege or the possibility to perform actions without technical traces or to deactivate or alter technical traces.
effective control	<p>a relationship constituted by rights, contracts or any other means which, either separately or jointly and having regard to the considerations of fact or law involved, confer the possibility of directly or indirectly exercising a decisive influence on an undertaking, in particular by:</p> <p>(a) the right to use all or part of the assets of an undertaking;</p> <p>(b) rights or contracts which confer a decisive influence on the composition, voting or decisions of the bodies of an under-taking or otherwise confer a decisive influence on the running of the business of the undertaking.</p> <p>Control is acquired by persons or undertakings which:</p> <p>(a) are holders of the rights or entitled to rights under contracts concerned; or</p> <p>(b) while not being holders of such rights or entitled to rights under such contracts, have the power to exercise the rights deriving therefrom.</p> <p>[SOURCE: Regulation (EC) No 139/2004 on the control of concentrations between undertakings, Article 3(2) and (3)]</p>
undertaking	<p>entities engaged in an economic activity, regardless of their legal status and the way in which they are financed including all linked enterprises or connected undertakings that form a group through the direct or indirect control of an enterprise or undertaking by another.</p> <p>[SOURCE: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Article 2(27)]</p>

J.2.1 PUA-01 Primacy of EU law

J.2.1.1 Objective

The CSP operates primarily within the legal framework provided by the EU and its Member States, with precedence over laws from non-EU states that may include extra-territorial measures.

J.2.1.2 Requirements

CS-EL1	The contracts between the CSPs and the CSCs related to the provision of the cloud service shall only be governed and construed by the law of an EU Member State, and shall (i) define, where possible under the governing law, one or multiple courts, tribunals or arbitration bodies from EU Member States that shall have jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract, and (ii) not confer jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract to any court, tribunal or arbitration body outside of EU Member States.	PUA-01.1B
CS-EL2	The contracts between the CSPs and the CSCs related to the provision of the cloud service shall only be governed and construed by the law of an EU Member State, and shall (i) define, where possible under the governing law, one or multiple courts, tribunals or arbitration bodies from EU Member States that shall have jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract, and (ii) not confer jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract to any court, tribunal or arbitration body outside of EU Member States.	PUA-01.1S
CS-EL3	The contracts between the CSPs and the CSCs related to the provision of the cloud service shall only be governed and construed by the law of an EU Member State, and shall (i) define, where possible under the governing law, one or multiple courts, tribunals or arbitration bodies from EU Member States that shall have jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract, and (ii) not confer jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract to any court, tribunal or arbitration body outside of EU Member States.	PUA-01.1H
	The CSP shall include in the risk assessment policies and procedures defined in RM-01 the risks related to non-EU laws with extra-territorial application that relate to the processing of CSC data and cloud service derived data that does not have the prior consent of the owner of the data, or is missing the prior consent of the legal persons mentioned in the data, and including at least: <ul style="list-style-type: none"> commercially sensitive and confidential information; and trade secrets. 	PUA-01.2H
	The CSP shall provide, upon demand from the CSC or prospective CSC, information allowing the CSC or prospective CSC to perform a risk assessment about the potential application of laws from a non-EU member state related to the processing of CSC data and cloud service derived data.	PUA-01.3H
	The CSP shall extend the requirements from PUA-02, PUA-03 and PUA-04 that apply to CSC data to all account data processed throughout the life cycle of the relationship between the CSP and the CSC (pre-sales, operation, maintenance and exit).	PUA-01.4H
	The CSP shall state in contractual documents with CSCs that the CSP shall only consider investigation requests related to the provision of the cloud service that are issued upon EU law or EU Member State law.	PUA-01.5H
CS-EL4	The contracts between the CSPs and the CSCs related to the provision of the cloud service shall only be governed and construed by the law of an EU Member State, and shall (i) define, where possible under the governing law, one or multiple courts, tribunals or arbitration bodies from EU Member States that shall have jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract, and (ii) not confer jurisdiction to settle any disputes which have arisen or which may arise in connection with that contract to any court, tribunal or arbitration body outside of EU Member States.	PUA-01.1H
	The CSP shall include in the risk assessment policies and procedures defined in RM-01 the risks related to non-EU laws with extra-territorial application that relate to the processing of	PUA-01.2H

CSC data and cloud service derived data that does not have the prior consent of the owner of the data, or is missing the prior consent of the legal persons mentioned in the data, and including at least:

- commercially sensitive and confidential information; and
- trade secrets.

The CSP shall provide, upon demand from the CSC or prospective CSC, information allowing the CSC or prospective CSC to perform a risk assessment about the potential application of laws from a non-EU member state related to the processing of CSC data and cloud service derived data.

PUA-01.3H

The CSP shall extend the requirements from PUA-02, PUA-03 and PUA-04 that apply to CSC data to all account data processed throughout the life cycle of the relationship between the CSP and the CSC (pre-sales, operation, maintenance and exit).

PUA-01.4H

The CSP shall state in contractual documents with CSCs that the CSP shall only consider investigation requests related to the provision of the cloud service that are issued upon EU law or EU Member State law.

PUA-01.5H

The CSP shall define and implement organisational and technical measures to ensure that investigation requests related to the provision of the cloud service that are not issued upon EU law or EU Member State law are not considered.

PUA-01.6H

J.2.1.3 Guidance requirements

- The guidance should define the evidence deemed acceptable for requirement PUA-01.1H (including sampling contracts, along with a binding statement from the CSP).
- About requirement PUA-01.2H, the scope of risk identification (from RM-01) should also specifically cover the aspects related to the risks on the confidentiality of customer data related to the use of other interested parties in the provision of the service (suppliers, subservice providers).
- About requirement PUA-01.3H, the objective would be to define a template for how this information has to be shared, with a minimum checklist.
- About requirement PUA-01.5H, the idea is that if the requesting country is not an EU Member State, then they should go through an EU Member State (e.g., through a legal assistance program) to get the information from the CSP.

J.2.2 PUA-02 Operation in the EU

J.2.2.1 Objective

The cloud service is operated and maintained from the EU, and all CSC data is stored and processed in the EU.

J.2.2.2 Requirements

CS-EL1	None	
CS-EL2	None	
CS-EL3	<p>The <u>CSP</u> shall include in the contractually available options for PSS-05.1 at least one option in which all locations indicated in <u>requirements</u> DOC-02.1H and DOC-02.2H are within the EU.</p> <p>The <u>CSP</u> shall only use in the provision of <u>trust services</u> that are being provided by a <u>Trusted Service Provider</u> based in an EU Member State.</p>	<p>PUA-02.1H</p> <p>PUA-02.2H</p>
CS-EL4	<p>All locations indicated by the <u>CSP</u> in <u>requirements</u> DOC-02.1H and DOC-02.2H shall be within the EU, with the following exceptions:</p> <ul style="list-style-type: none"> When some support activities are performed outside of the EU, the <u>CSP</u> shall list all the activities performed outside of the EU. In addition to the support activities defined above, but not including any administration activities and supervision activities some activities may be performed outside of the EU in exceptional circumstances to be defined in the contractual agreements with the <u>CSCs</u> and the <u>CSP</u> shall offer an option to their <u>CSCs</u> to guarantee that all activities are always performed in the EU. <p>The <u>CSP</u> shall only use in the provision of <u>trust services</u> that are being provided by a <u>Trusted Service Provider</u> based in an EU Member State.</p>	<p>PUA-02.1H</p> <p>PUA-02.2H</p>

J.2.2.3 Guidance requirements

- Requirement PUA-02.1H is a refinement of requirement PSS-05.1S that simply requires the availability of an option for all processing and storage to take place in the EU.
- PUA-02.1H is a refinement of PUA-02.1S in the sense that it is much stronger (all options must be in the EU, instead of at least one).
- Requirement PSS-05.2H applies to the location commitments in PUA-02.1H.
- For PUA-02.2H, the essential trust service to be considered is the issuance and maintenance of PKI digital certificates.
- For PUA-02.2H, the master key generation ceremonies should be performed in the EU, in the presence of a representative of the CSP.

J.2.3 PUA-03 Controlling exchanges with employees and suppliers outside of the EU

J.2.3.1 Objective

The exchanges between the cloud service and its employees and suppliers are controlled specifically when the employee or supplier is located outside of the EU.

J.2.3.2 Requirements

CS-EL1	None	
CS-EL2	None	
CS-EL3	<p>Before granting to an <u>employee</u> with direct or indirect access to <u>CSC data</u>, including in support operations, the <u>CSP</u> shall verify that the <u>employee</u> performing the action is located in the EU or is supervised as defined in IAM-09.8H by an <u>employee</u> who passed an appropriate review (cf.IAM-09.7H) and is located in the EU.</p> <p>In the context of support of a functional component used in the provision of the cloud service, considering the <u>risks</u> on the confidentiality of <u>CSC data</u>, prior to allowing an access, the <u>CSP</u> shall:</p> <ul style="list-style-type: none"> • verify that the person performing the action has passed an appropriate review and is located in the EU, or is supervised by a <u>CSP employee</u> who has passed an appropriate review (cf. HR-02.1H) and is located in the EU; • in case of supervised access, verify that the access is performed using a secure solution that allows the supervising employee to authorize or forbid individual actions, and to ask for explanations, in real time; <p>All actions performed related to the maintenance of a functional component used in the provision of the cloud service shall be logged as administrative actions, monitored, properly concluded, and archived.</p>	<p>PUA-03.1H</p> <p>PUA-03.2H</p> <p>PUA-03.3H</p>
CS-EL4	<p>Before granting to an <u>employee</u> direct or indirect access to <u>CSC data</u>, including in support operations, the <u>CSP</u> shall verify that the <u>employee</u> performing the action is located in the EU or is supervised as defined in IAM-09.8H by an <u>employee</u> who passed an appropriate review (cf.IAM-09.7H) and is located in the EU.</p> <p>In the context of support of a functional component used in the provision of the cloud service, considering the <u>risks</u> on the confidentiality of <u>CSC data</u>, prior to allowing an access, the <u>CSP</u> shall:</p> <ul style="list-style-type: none"> • verify that the person performing the action has passed an appropriate review and is located in the EU, or is supervised by a <u>CSP employee</u> who has passed an appropriate review (cf. HR-02.1H) and is located in the EU; • in case of supervised access, verify that the access is performed using a secure solution that allows the supervising employee to authorize or forbid individual actions, and to ask for explanations, in real time; <p>All actions performed related to the maintenance of a functional component used in the provision of the cloud service shall be logged as administrative actions, monitored, properly concluded, and archived.</p>	<p>PUA-03.1H</p> <p>PUA-03.2H</p> <p>PUA-03.3H</p>

J.2.3.1 Guidance requirements

None

J.2.4 PUA-04 Control requirements

J.2.4.1 Objective

Certified cloud services are operated only by companies based in the EU, with no entity from outside the EU having effective control over the CSP, to mitigate the risk of non-EU interfering powers undermining EU regulations, norms and values.

J.2.4.2 Requirements

CS-EL1	None	
CS-EL2	None	
CS-EL3	None	
CS-EL4	<p>The CSP's registered head office and global headquarters shall be established in a Member State of the EU.</p> <p>Undertakings whose registered head office or headquarters are not established in a Member State of the EU shall not, directly or indirectly, solely or jointly, hold positive or negative effective control of the CSP applying for the certification of a cloud service.</p>	<p>PUA-04.1H</p> <p>PUA-04.2H</p>

J.2.4.1 Additional information

A definition of the notion "control" (renamed "effective control" here to avoid confusion with the other use of the term control in the EUCS) provided in Article 3(2) and (3) of Regulation 139/2004 shall be used for the assessment of the conformity to eligibility requirement PUA-04.2H, namely:

2. Control shall be constituted by rights, contracts or any other means which, either separately or in combination and having regard to the considerations of fact or law involved, confer the possibility of exercising decisive influence on an undertaking, in particular by:

- (a) ownership or the right to use all or part of the assets of an undertaking;
- (b) rights or contracts which confer decisive influence on the composition, voting or decisions of the organs of an undertaking.

3. Control is acquired by persons or undertakings which:

- (a) are holders of the rights or entitled to rights under contracts concerned; or
- (b) while not being holders of such rights or entitled to rights under such contracts, have the power to exercise the rights deriving therefrom.

Regulation 139/2004 is enforced by the Commission and the Member States, by governmental entities which have access to the required information and competence. For the EUCS, the assessment of the conformity to eligibility requirements PUA-04.1H and PUA-04.2H shall be performed in each country by CABs issuing certificates at assurance level 'high', and these activities shall be covered by the EUCS peer review and peer assessment mechanisms to guarantee the harmonization of their assessment criteria and activities.

NOTE: Since these activities are relative to certification at assurance level 'high', they remain under the ultimate responsibility of the NCCA, which may organise this activity with the collaboration of other government entities.

J.2.4.2 *Guidance requirements*

- Additional guidance should be provided to CSPs about requirements PUA-04.1H+ and PUA-04.2H+, complementing existing guidelines and case-law already available for Regulation 139/2004 or related regulations.
- The guidance should define the evidence deemed acceptable for the assessment of the conformity to eligibility requirement PUA-04.1H+ (including certificate of registration, proof of principal functionality and operation control)
- The guidance should define the evidence deemed acceptable for the assessment of the conformity to eligibility requirement PUA-04.2H+ (including applicable legislation relating to exercise of effective control over undertaking, binding statement from the CSP on ownership structure).

POLITICO

ANNEX K: 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

POLITICO

K.1 INTRODUCTION

The terminology draws from a large number of sources, including ISO standards (ISO/IEC 17000, ISO/IEC 17021-1, ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 22123-1), IAASB documentation, and EU regulations.

In addition, the terminology defines derived terms, such as a verb defined as the performance of an action for which a noun is defined, and it also includes a number of specific terms that are used mostly in the definition of the service requirements in Annex A: (Security Objectives and requirements for Cloud Services).

K.2 MAIN TERMINOLOGY

Term	Definition
access control	means to ensure that physical and logical access to <u>assets</u> is authorised and restricted based on business and information security <u>requirements</u> [SOURCE: From ISO/IEC 27002:2022, 3.1.1]
access right	permission for a subject to access a particular object for a specific type of operation [SOURCE: From ISO/IEC 2382:2015, 2126298]
account data	class of data specific to each <u>cloud service customer</u> that is required to administer the <u>cloud service</u> Note 1 to entry: Account data is typically generated when a <u>cloud service</u> is purchased and is under the <u>control</u> of the <u>cloud service provider</u> . Note 2 to entry: Account data consists of data elements provided by the <u>cloud service customer</u> , such as; name, address, telephone, etc. [SOURCE: From ISO/IEC 22123-1:2021(en), 3.10.4]
accreditation	third-party <u>attestation</u> related to a <u>conformity assessment body</u> , conveying formal demonstration of its competence, impartiality and consistent operation in performing specific <u>conformity assessment activities</u> [SOURCE: From ISO/IEC 17000:2020(en), 7.7]
accreditation body	<u>conformity assessment body</u> that performs <u>accreditation</u> Note 1 to entry: The authority of an accreditation body is generally derived from government. [SOURCE: From ISO/IEC 17000:2020(en), 2.6]
activity	specified pursuit or set of tasks [SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.8]
anonymization	process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party [SOURCE: From ISO/IEC 29100:2011(en), 2.2]
application capabilities type	<u>cloud capabilities type</u> in which the <u>cloud service customer</u> can use the <u>cloud service provider's applications</u> [SOURCE: From ISO/IEC 22123-1:2021(en), 3.6.2]
application document	the document provided by a CSP to the CAB when applying for <u>certification</u> , which provides information about the <u>cloud service</u> to be <u>certified</u>
appropriateness of evidence	The measure of the quality of <u>evidence</u> [SOURCE: From ISAE3000: 12.i.i]

Term	Definition
asset	<p>anything that has value to the organization</p> <p>Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:</p> <ul style="list-style-type: none"> — the primary assets: — information; — business processes and activities; — the supporting assets (on which the primary assets rely) of all types, for example: — hardware; — software; — network; — personnel; — site; — organization's structure. <p>[SOURCE: From ISO/IEC 27002:2022(en), 3.1.2]</p>
asset life	<p>period from asset creation to asset end-of-life</p> <p>[SOURCE: From ISO 55000:2014(en), 3.2.2]</p>
asset system	<p>set of assets that interact or are interrelated</p> <p>[SOURCE: From ISO 55000:2014(en), 3.2.5]</p>
assumption	<p>a factor in the conformity assessment process that is considered to be true, real, or certain, without proof or demonstration</p> <p>[From ISO/IEC/IEEE 24765:2017(en), 3.276]</p>
assurance	<p>grounds for justified confidence that a product, service or process meets specified requirements</p> <p>[SOURCES: Inspired from ISO/IEC 15408-1:3(2009).1.4 and from ISO/IEC/IEEE 15026-1(2019):3.1]</p>
assurance claim	<p>assertion or supporting assertion that a system meets a stated security need</p> <p>Note 1 to entry: Claims address both direct threats (e.g. system data are protected from attacks by outsiders) and indirect threats (e.g. system code has minimal flaws).</p> <p>Note 2 to entry: Compare with the definition of "claim".</p> <p>[SOURCE: From ISO/IEC TR 15443-1:2012, 3.10]</p>
assurance information	<p>information including a claim about a system, evidence supporting the claim, an argument showing how the evidence supports the achievement of the claim, and the context for these items</p> <p>[SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]</p>
assurance level	<p>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</p> <p>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.</p> <p>[SOURCE: From EC 881/2019, 2.21]</p>
attestation	<p>issue of a statement, based on a decision, that fulfilment of specified requirements has been demonstrated</p> <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>

Term	Definition
	[SOURCE: From ISO/IEC 17000:2020(en), 5.2]
audit	systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled [SOURCE: From ISO 19011:2018(en), 3.1]
audit conclusion	outcome of an audit, after consideration of the audit objectives and all audit findings [SOURCE: From ISO 9000:2015, 3.13.10]
audit criteria	set of requirements used as a reference against which objective evidence is compared Note 1 to entry: Requirements may include policies, procedures , work instructions, legal requirements , contractual obligations, etc. [SOURCE: ISO 19011:2018(en), 3.7]
audit evidence	records, statements of fact or other information, which are relevant to the audit criteria and verifiable [SOURCE: FROM ISO/IEC 19011:2018, 3.9]
audit findings	results of the evaluation of the collected audit evidence against audit criteria [SOURCE: FROM ISO/IEC 19011:2018, 3.10]
audit plan	description of the activities and arrangements for an audit [SOURCE: From ISO 9000:2015, 3.13.6]
audit programme	arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose [SOURCE: ISO 19011:2018, 3.4]
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: ISO 9000:2015(en), 3.13.14]
audit time	time needed to plan and accomplish a complete and effective audit of the client's service [SOURCE: From ISO/IEC 17021-1:2015, 3.16]
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 ISO/IEC 17021-1:2015(en), 3.6]
authorised body	person or group of persons to whom top management has delegated a task or responsibility NOTE: In security controls, authorized bodies would typically be responsible for of a given policy and related procedures
authorisation	activity performed by a NCCA to verify that an accredited CAB meets the specific or additional requirements define in a European cybersecurity certification scheme [SOURCE: From EUCSA, Article 60(3)]
bridge letter	A document made available by a service organisation to cover a period of time between the reporting period end date of the current ISAE report and the release of a new ISAE report. Note to entry: bridge letters are needed in complements to ISAE reports that do not make forward-looking statements, to provide some guarantee that the vendor still operates the controls that have been audited in the previous reports, and declares any changes to its control framework [SOURE: ISAE]

Term	Definition
business continuity	capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption [SOURCE: From ISO 22301:2019(en), 2019, 3.3]
business continuity plan	documented information that guides an organization to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives [SOURCE: From ISO 22301:2019(en), 2019, 3.4]
business impact analysis	process of analysing the impact over time of a disruption on the organization Note 1 to entry: The outcome is a statement and justification of business continuity requirements. [SOURCE: From ISO 22301:2019(en), 2019, 3.5]
capacity management	process for monitoring, analysis, reporting and improvement of capacity [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.2]
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]
certification	third-party attestation related to an object of conformity assessment, with the exception of accreditation [SOURCE: From ISO/IEC 17000:2020(en), 7.6]
certification audit joint audit combined audit integrated audit	audit carried out by an auditing organization independent of the client and the parties that rely on certification, for the purpose of certifying the client's service Note 1 to entry: Unless specifically qualified (e.g., "internal audit"), in the definitions which follow, the term "audit" has been used for simplicity to refer to third-party certification audit. Note 2 to entry: Certification audits include initial, surveillance, re-certification audits, and can also include special audits. Note 3 to entry: A joint audit is when two or more auditing organizations cooperate to audit a single client. Note 4 to entry: A combined audit is when a client is being audited against the requirements of two or more standards together. Note 5 to entry: An integrated audit is when a client has integrated the application of requirements of two or more standards into a single service and is being audited against more than one standard. Note 6 to entry: Removed references to management systems and the original Note 3. [SOURCE: From ISO/IEC 17021-1:2015, 3.4]
certification body	third-party conformity assessment body that performs review and certification activities.
certification report	the document that accompanies the certificate, and provides a simple presentation of the cloud service and a summary of the conformity assessment activities
certification requirement	specified requirement, including service requirements, that is fulfilled by the client as a condition of establishing or maintaining certification Note to entry: This is the most high-level definition, which covers all kinds of requirements that need to be met in order to be certified. [SOURCE: From ISO/IEC 17065:2012, definition 3.7]
certification scheme	conformity assessment scheme that includes a certification activity

Term	Definition
	Note 1 to entry: In a certification scheme, a successful assessment leads to the issuance of a certificate.
certified cloud service	a cloud service that that has been awarded an EUCS certificate that is still valid, and whose CSP continues to fulfil the EUCS requirements Note 1 to entry: This is a restrictive definition in use solely in the EUCS scheme
change management	process for recording, coordination, approval and monitoring of all changes [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.3]
characteristic	distinguishing feature Note 1 to entry: A characteristic can be inherent or assigned. Note 2 to entry: A characteristic can be qualitative or quantitative. [SOURCE: From ISO 9000:2015(en), 3.10.1]
claim	statement of something to be true including associated conditions and limitations Note 1 to entry: The statement of a claim does not mean that the only possible intent or desire is to show it is true. Sometimes claims are made for the purpose of evaluating whether they are true or false or undertaking an effort to establish what is true. Note 2 to entry: In its entirety, a claim conforming to ISO/IEC 15026-2 is an unambiguous declaration of an assertion with any associated conditionality giving explicit details including limitations on values and uncertainty. It could be about the future, present, or past. [SOURCE: From ISO/IEC 15026-1:2010(en), 2.4]
client	organization whose service is being audited for certification purposes Note 1 to entry: "management system" has been replaced by "service" [SOURCE: Adapted from ISO/IEC 17021-1:2015(en), 3.5]
cloud capabilities type	classification of the functionality provided by a cloud service to the cloud service customer , based on resources used Note 1 to entry: The cloud capabilities types are application capabilities type , infrastructure capabilities type and platform capabilities type . [SOURCE: From ISO/IEC 22123-1:2021(en), 3.6.1]
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 Note 1 to entry: Examples of resources include servers, operating systems , networks, software, applications, and storage equipment. [SOURCE: From ISO/IEC 22123-1:2021(en), 3.2.1]
cloud deployment model	way in which cloud computing can be organized based on the control and sharing of physical or virtual resources Note 1 to entry: The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud. [SOURCE: From ISO/IEC 22123-1:2021(en), 3.3.1]
cloud service	one or more capabilities offered via cloud computing invoked using a defined interface [SOURCE: From ISO/IEC 22123-1:2021(en), 3.2.2]
cloud service customer CSC	party which is in a business relationship for the purpose of using cloud services [SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.2]
cloud service customer data CSC 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

Term	Definition
	<p>obtained from another source, or it might be publicly available 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.</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.10.1]</p>
cloud service derived data	<p>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</p> <p>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.</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.10.2]</p>
cloud service developer	<p>cloud service partner with the responsibility for designing, developing, testing and maintaining the implementation of a cloud service</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.14]</p>
cloud service extension profile extension profile CSEP	<p>A document defining extended requirements to complement the EUCS in a specific security context</p>
cloud service extension profile developer CSEP developer	<p>the role of an entity in charge of the development of a CSEP</p> <p>Note: Various entities can take this role, including private companies, industry associations, or a National or European institution like a NCCA or ENISA</p>
cloud service provider CSP	<p>party which makes cloud services available</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.3]</p>
cloud service provider data CSP data	<p>class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider</p> <p>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.</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.10.3]</p>
cloud service user	<p>natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services</p> <p>NOTE: Examples of such entities include devices and applications.</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.4]</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>
competence	<p>ability to apply knowledge and skills to achieve intended results</p> <p>[SOURCE: From ISO/IEC 17021:2015(en), 3.7]</p>
complaint	<p>expression of dissatisfaction by any person or organization to a CAB or accreditation body or to the CAB's NCCA, relating to the activity of that CAB, where a response is expected</p> <p>[SOURCE: Adapted from ISO/IEC 17000:2020, 8.7]</p>
complementary user entity controls CUEC	<p>the controls that the CSP assumes that their CSCs will have in place in order for them to securely use their cloud service</p> <p>NOTE: The term originates from the audit community, which is why it refers to a user entity instead of a customer, but the meaning is the same.</p> <p>[SOURCE: SOC2]</p>

Term	Definition
complementary service organization controls CSOC	the controls that the CSP assumes that their <u>subservice providers</u> will have in place in order for them to securely operate their cloud service NOTE: The term originates from the audit community, which is why it refers to a subservice organization instead of a <u>subservice provider</u> , but the meaning is the same. [SOURCE: SOC2]
compliance	conformity in the context of the rules and requirements defined in a <u>certification scheme</u> that apply to the provider of the certified product, service or process Note 1 to entry: This is a refinement of ISO19011, which defines compliance as <u>conformity</u> in the context of a statutory requirement or regulatory requirement. In this case, compliance is <u>conformity</u> in the context of a given scheme. Note 2 to entry: The term is used to differentiate between compliance of a cloud service provider to the requirements defined in the scheme and <u>conformity</u> of a <u>cloud service</u> to the requirements on <u>controls</u> defined in the scheme. [SOURCE: Inspired from ISO 19011:2018(en), 3.7]
composition	reuse of the results of <u>certification activities</u> of a <u>certified cloud service</u> in the <u>evaluation</u> of a <u>primary cloud service</u> using that <u>certified cloud service</u> as <u>secondary cloud service</u>
compromise	Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of <u>svstems</u> or (2) the integrity or availability of <u>svstem inputs</u> or <u>outputs</u> [SOURCE: TSC]
configuration management	<u>process</u> for logging and monitoring of configuration items [SOURCE: From ISO/IEC TS 22237-7:2018(en), 3.1.5]
conformity	fulfilment of a <u>requirement</u> Note 1 to entry: when used in opposition with compliance, conformity relates to the requirements related to the object of <u>conformity assessment</u> rather than to the <u>requirements</u> related to the certification scheme. [SOURCE: From ISO Supplement:3.18]
conformity assessment	demonstration that <u>specified requirements</u> are fulfilled Note 1 to entry: The <u>process</u> of <u>conformity assessment</u> (...) can have a negative outcome, i.e. demonstrating that the <u>specified requirements</u> are not fulfilled. Note 1 to entry: The subject field of conformity assessment includes <u>selection activities</u> , <u>determination activities</u> such as <u>testing</u> , <u>inspection</u> and <u>audit</u> , <u>review activities</u> , and <u>attestation activities</u> such as <u>certification</u> , as well as the <u>accreditation</u> of <u>conformity assessment bodies</u> . Note 3 to entry: [ISO17000] does not include a definition of “ <u>conformity</u> ”. “ <u>Conformity</u> ” does not feature in the definition of “ <u>conformity assessment</u> ”. Nor does [ISO17000] address the concept of compliance. [SOURCE: From ISO/IEC 17000:2020(en), 4.1, some modifications in notes]
conformity assessment body CAB	body that performs <u>conformity assessment services</u> [SOURCE: From ISO/IEC 17000:2020(en), 2.5]
conformity assessment scheme	<u>conformity assessment system</u> related to specified objects of <u>conformity assessment</u> , to which the same <u>specified requirements</u> , specific rules and <u>procedures</u> apply [SOURCE: From ISO/IEC 17000:2020(en), 2.8]
conformity assessment system	rules, procedures and management for carrying out <u>conformity assessment</u> Note 1 to entry: The Cybersecurity Act is a conformity assessment system from which are derived <u>European cybersecurity certification schemes</u> . [SOURCE: From ISO/IEC 17000:2020(en), 2.7]
conformity self-assessment	<u>first-party conformity assessment activities</u> , which evaluate whether those <u>ICT products</u> , <u>ICT services</u> or <u>ICT processes</u> meet the <u>requirements</u> of a specific <u>European cybersecurity certification scheme</u>

Term	Definition
	<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>
consultancy	<p>participation in</p> <p>a) the designing, manufacturing installing, maintaining or distributing of a certified product or a product to be certified, or</p> <p>b) the designing, implementing, operating or maintaining of a certified process or a process to be certified, or</p> <p>c) the designing, providing or maintaining of a certified service or a service to be certified</p> <p>[SOURCE: From ISO/IEC 17065:2012, 3.2]</p>
control	<p>measure that maintains and/or modifies 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/IEC 27002:2022(en), 3.1.8]</p>
control objective	<p>statement describing what is to be achieved as a result of implementing controls</p> <p>[SOURCE: ISO/IEC 27000:2018(en), 3.15]</p>
control risk	<p>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</p>
credential	<p>representation of an identity</p> <p>Note 1 to entry: A credential is typically made to facilitate data authentication of the identity information in the identity it represents.</p> <p>Note 2 to entry: The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid.</p> <p>EXAMPLE: A credential can be a username, a username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.</p> <p>[SOURCE: From ISO/IEC 24760-1:2011, 3.3.5]</p>
criteria	<p>rules on which a judgment or decision can be based, or by which a product, service, result, or process (3.1.20) can be evaluated</p> <p>[SOURCE: From ISO/IEC/IEEE 15289:2019(en), 3.1.6]</p>
Cybersecurity Act EUCSA	<p>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</p>
data at rest	<p>structure, or group of structures, dedicated to the centralized accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability</p> <p>Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function.</p> <p>Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building.</p> <p>[SOURCE: From ISO/IEC 30134-1:2016(en), 3.6]</p>
data centre	<p>location hosting the equipment from which the cloud service operates</p>
data in motion	<p>data being transferred from one location to another</p>

Term	Definition
	Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device). [SOURCE: From ISO/IEC 27040:2015(en), 3.8]
decision	conclusion, based on the results of review, that fulfilment of <u>specified requirements</u> has or has not been demonstrated [SOURCE: From ISO/IEC 17000:2020(en), 7.2]
declaration	<u>first-party attestation</u> [SOURCE: From ISO/IEC 17000:2020(en), 7.5]
de-identification process	process of removing the association between a set of identifying attributes and the data principal [SOURCE : From ISO/IEC 20889:2018(en), 3.6]
demilitarized zone DMZ	perimeter network (also known as a screened sub-net) inserted as a “neutral zone” between networks [SOURCE: From ISO/IEC 27033-1:2015(en), 3.8]
design effectiveness	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 (i) the risks that threaten the achievement of the <u>control objectives</u> have been identified by management; (ii) the controls would, if operating effectively, provide reasonable assurance that those risks would not prevent the <u>control objectives</u> from being achieved. [SOURCE: Inspired from ISAE3402]
detective control	A <u>control</u> that detects and reports when errors, omissions and unauthorized uses or entries occur [SOURCE: SOC2]
determination	activities undertaken to develop complete information regarding fulfilment of the <u>specified requirements</u> by the object of <u>conformity assessment</u> or its sample [SOURCE: From ISO/IEC 17000:2020(en), A.3.1]
development environment	The environment in which changes to software are developed NOTE: The environment may be local to an individual developer’s workstation or distributed, possibly based on external <u>services</u>
disruption	incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of <u>products</u> and <u>services</u> according to an organization’s objectives [SOURCE: From ISO 22301:2019(en), 2019, 3.10]
document	recorded information or material object, which can be treated as a unit [SOURCE: From ISO 5127:2001, 1.2.02]
effectiveness	extent to which planned <u>activities</u> are realized and planned results achieved [SOURCE: ISO Supplement:3.6]
employee	a person under employment contract with the CSP to whom human resource management controls apply
EU statement of conformity	declaration produced by a vendor of ICT product, ICT process, or ICT service after performing a <u>conformity self-assessment</u> in the context of an European cybersecurity certification scheme, that states that a specific ICT product, ICT service or ICT process complies with the <u>requirements</u> of the <u>European cybersecurity certification scheme</u>

Term	Definition
European Cybersecurity Certification group ECCG	A group composed of representatives of national cybersecurity certification authorities or other relevant national authorities [SOURCE: Adapted from Cybersecurity Act , Article 62]
European cybersecurity certification scheme EUCS	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]
evaluation	combination of the selection and determination functions of conformity assessment activities [SOURCE: From ISO/IEC 17065:2012(en), 3.3]
evaluation level	a combination of assurance components within an evaluation methodology that corresponds to an assurance level and appropriate level of depth and rigour, corresponding to a category of security problems [SOURCE: From EC 881/2019, 52.8]
evaluation report	the document written by the CAB to describe the evaluation activities and their results, including the audit and the dependency analysis
events log	log which records audit trail data related to the system operations [SOURCE: From ISO 14641:2018, 3.2]
expiry	ending of the validity of the statement of conformity after a specified period [SOURCE: From ISO/IEC 17000:2020(en), 8.4]
extended requirement	a service requirement defined in a CSFP
feature	abstract functional characteristic of a system of interest that end-users and other stakeholders can understand Note 1 to entry: In systems engineering, features are syntheses of the needs of stakeholders. These features will be used, amongst others, to build the technical requirement baselines. [SOURCE: From ISO/IEC 26550:2015(en), 3.14]
first-party	the person or organization that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020(en), 2.2]
first-party conformity assessment activity	conformity assessment activity that is performed by the person or organization that provides the object of conformity assessment [SOURCE: From ISO/IEC 17000:2020(en), 4.3]
functional component	functional building block needed to engage in an activity , backed by an implementation [SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.10]
guide	person appointed by the client to assist the audit team [SOURCE: From ISO/IEC 17021-1:2011, 3.8]
headquarters	the head office or the registered office of the undertaking within which the principal financial functions and operational control are exercised [SOURCE: Adapted from Data Act]
ICT process	a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service

Term	Definition
	<p>Note 1 to entry: This term is to be used when a <u>process</u> is intended to be the object of a cybersecurity <u>certification</u>. The term '<u>process</u>' is more general and should be used in other situations.</p> <p>[SOURCE: From EC881/2019:2.14]</p>
ICT product	<p>an element or a group of elements of a network or information system</p> <p>Note 1 to entry: In the definition of <u>certification schemes</u>, the use of 'ICT product' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and <u>products</u> certified using such schemes. It is a subset of the more general term <u>product</u>, whose definition originates in ISO9000.</p> <p>[SOURCE: From EC881/2019:2.12]</p>
ICT service	<p>a service consisting fully or mainly in the transmission, storing, retrieving or <u>processing</u> of information by means of network and information <u>systems</u></p> <p>Note 1 to entry: In the definition of <u>certification schemes</u>, the use of 'ICT service' follows this definition from EC 881-2019, and will mostly be used to refer to certification schemes and <u>products</u> certified using such schemes. For a more general use, it is preferable to use the term 'service'.</p> <p>[SOURCE: From EC881/2019:2.13]</p>
impact	<p>outcome of a disruption affecting objectives</p> <p>[SOURCE: From ISO 22301:2019(en), 3.10]</p>
impartiality	<p>presence of objectivity</p> <p>[SOURCE: From ISO/IEC 17065:2012, 3.13]</p>
incident handling	<p>actions of detecting, reporting, assessing, responding to, dealing with, and learning from information <u>security incidents</u></p> <p>[SOURCE: From ISO/IEC 27035-1:2016, 3.6]</p>
incident response	<p>actions taken to mitigate or resolve an information <u>security incident</u>, including those taken to protect and restore the normal operational conditions of an information <u>system</u> and the information stored in it</p> <p>[SOURCE: From ISO/IEC 27035-1:2016, 3.7]</p>
information security	<p>preservation of confidentiality, integrity and availability of information</p> <p>[SOURCE: From ISO/IEC 27000:2016, 2.33]</p>
information security event security event	<p>occurrence indicating a possible breach of information security or failure of <u>controls</u></p> <p>[SOURCE: From ISO/IEC 27035-1:2016, 3.3]</p>
information security incident security incident incident	<p>one or multiple related and identified information security events that can harm an organization's <u>assets</u> or <u>compromise</u> its operations</p> <p>[SOURCE: From ISO/IEC 27035-1:2016, 3.4]</p>
information security management system ISMS	<p>part of the overall <u>management system</u>, based on a business <u>risk</u> approach, used to establish, implement, operate, monitor, review, maintain and improve information security</p> <p>[SOURCE: From ISO/TS 12812-2:2017(en), 3.11]</p>
inclusive method	<p>Method of dealing with the services provided by a subservice organization, whereby the service organization's description of its <u>system</u> 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 <u>system</u> and in the scope of the service auditor's engagement</p> <p>[SOURCE: From ISAE3402: 9.g]</p>
information	<p>meaningful data</p> <p>[SOURCE: ISO 9000:2015, 3.8.2]</p>

Term	Definition
information service	<p>any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.</p> <p>Note 1 to entry: For the purposes of this definition:</p> <p>(i) 'at a distance' means that the <u>service</u> is provided without the parties being simultaneously present;</p> <p>(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;</p> <p>(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.</p> <p>[SOURCE: From EC1535/2015:1.b]</p>
infrastructure capabilities type	<p>cloud capabilities type in which the <u>cloud service customer</u> can provision and use <u>processing</u>, storage or networking resources</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.6.4]</p>
inquiry	<p>activity consisting of seeking information of knowledgeable persons, within the entity or outside the entity</p> <p>[SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]</p>
inspection	<p>an activity involving the examination of records or documents, whether internal or external, in paper form, electronic form, or on other media, or a physical examination of evidence</p> <p>[SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]</p>
inter-cloud computing	<p>paradigm for enabling the interworking between two or more <u>cloud service providers</u>.</p> <p>[SOURCE: From ISO/IEC 22123-1:2021(en), 3.12.1]</p>
interested party stakeholder	<p>person or organization that can affect, be affected by, or perceive itself to be affected by a decision or <u>activity</u></p> <p>[SOURCE: ISO Supplement:3.2]</p>
internal audit	<p><u>audit</u> where the <u>audit team</u> belongs to the <u>auditee</u></p> <p>[SOURCE: From ISO 14050:2020(en), 3.4.40]</p>
laboratory	<p>body that performs one or more of the following <u>activities</u>:</p> <ul style="list-style-type: none"> - <u>testing</u>; - calibration; - <u>sampling</u>, associated with subsequent <u>testing</u> and calibration <p>[SOURCE: From ISO/IEC 17025:2017, 3.6]</p>
life cycle	<p>stages involved in the management of an <u>asset</u></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 ISO 55000:2014(en), 3.2.3]</p>
major nonconformity	<p><u>nonconformity</u> that affects the capability of the <u>management system</u> to achieve its intended results</p> <p>Note 1 to entry: Nonconformities could be classified as major in the following circumstances:</p> <ul style="list-style-type: none"> - if there is a significant doubt that effective <u>process control</u> is in place, or that <u>products</u> or <u>services</u> will meet <u>specified requirements</u>; - a number of minor nonconformities associated with the same <u>requirement</u> or <u>issue</u> could demonstrate a <u>systemic failure</u> and thus constitute a <u>major nonconformity</u>. <p>[SOURCE: Adapted from ISO/IEC 17021-1:2015(en), 3.12]</p>

Term	Definition
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: ISO 9000:2015(en), 3.5.3]</p>
measured service	<p>metered delivery of cloud services such that usage can be monitored, controlled, reported and billed</p> <p>[SOURCE: ISO/IEC 22123-1:2021(en), 3.5.1]</p>
minor nonconformity	<p>nonconformity that does not affect the capability of the management system to achieve its intended results</p>
monitoring	<p>determining the status of a system, a process or an activity</p> <p>Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.</p> <p>[SOURCE: ISO/IEC 27000:2018(en), 3.46]</p>
multi-tenancy	<p>allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another</p> <p>[SOURCE: ISO/IEC 22123-1:2021(en), 3.5.3]</p>
national cybersecurity certification scheme national scheme	<p>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</p> <p>Note 1 to entry: This definition is a refinement of the definition of a certification scheme.</p> <p>[SOURCE: From EC 881/2019:2.10]</p>
national accreditation body NAB	<p>the sole body in a Member State that performs accreditation with authority derived from the State</p> <p>[SOURCE: From EC765/2008:2.1]</p>
non-compliance	<p>nonconformity in the context of the rules and requirements defined in a certification scheme</p> <p>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.</p> <p>[SOURCE: Inspired from ISO 19011:2018(en), 3.7]</p>
nonconformity	<p>non-fulfilment of a requirement</p> <p>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.</p> <p>[SOURCE: From ISO Supplement:3.19]</p>
object of conformity assessment object	<p>entity to which specified requirements apply</p> <p>EXAMPLE: Product, process, service, system, installation, project, data, design, material, claim, person, body or organization, or any combination thereof.</p> <p>[SOURCE: From ISO/IEC 17000:2020(en), 4.2, Note 2]</p>
objective	<p>result to be achieved</p> <p>Note 1 to entry: An objective can be strategic, tactical, or operational.</p>

Term	Definition
	<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 ISO/IEC 27000:2018(en), 3.49]</p>
objective evidence 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 ISO 9000:2015(en), 3.8.3]</p>
observation	<p>activity consisting of looking at a process or procedure being performed by others</p> <p>[SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]</p>
observer	<p>person who accompanies the audit team but does not audit</p> <p>[SOURCE: From ISO/IEC 17021-1:2015(en), 3.9]</p>
on-demand self-service	<p>feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider</p> <p>[SOURCE: ISO/IEC 22123-1:2021(en), 3.5.1]</p>
operating effectiveness	<p>A control is operating effectively, if</p> <p>(i) it was consistently applied as designed throughout the specified period, and</p> <p>(ii) in case of manual controls, they were applied by individuals who have the appropriate competence and authority.</p> <p>[SOURCE: Inspired from ISAE3402]</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 ISO/IEC 17065:2012(en), 3.8]</p>
operational risk	<p>A risk arising from execution of a company's business functions</p>
organization	<p>person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives</p> <p>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.</p> <p>[SOURCE: ISO Supplement:3.1]</p>
output	<p>result of a process</p> <p>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.</p> <p>[SOURCE: From ISO 9000:2015(en), 5.6]</p>
outsourcing	<p>acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's</p> <p>[SOURCE: From ISO/IEC 27036-1:2015, 3.6]</p>

Term	Definition
peer assessment	assessment of a body against <u>specified requirements</u> by representatives of other bodies in, or candidates for, an agreement group 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. Note 2 to entry: On the other hand, this could cover both CABs at level 'high' and NCCAs, but some rewriting is required. [SOURCE: From ISO/IEC 17000:2020(en), 4.5]
penetration testing	Authorized simulated cyberattack on a computer <u>system</u> , performed to evaluate the security of the <u>system</u> . [SOURCE: Adapted from Wikipedia]
personnel	persons doing work under the CSP's direction Note 1 to entry: The concept of personnel includes the CSP's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers. [SOURCE: Adapted from ISO/IEC 27002:2022, 3.1.20]
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 <u>supported by the cloud service provider</u> [SOURCE: From ISO/IEC 22123-1:2021(en), 3.6.4]
point of contact	defined organizational function or role serving as the coordinator or focal point of information concerning <u>incident management activities</u> [SOURCE: From ISO/IEC 27035-1:2016, 3.8]
policy	intentions and direction of an organization, as formally expressed by its <u>top management</u> [SOURCE: ISO Supplement, 3.7]
predictive assurance	recognition of the vendor's consistent repeatability to provide deliverables that satisfy its security <u>policy</u> or to perform as claimed [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.19]
pre-production environment	Mirror of <u>production environment</u> used for final <u>testing</u> or debugging
preventive control	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 <u>process</u> or end product [SOURCE: SOC2]
primary cloud service	In inter-cloud computing, the cloud service offered by a <u>primary cloud service provider</u> [SOURCE: Derived from ISO/IEC 22123-1:2021(en), 3.12.2]
primary cloud service provider	In <u>inter-cloud computing</u> , a <u>cloud service provider</u> which is making use of <u>cloud services</u> of <u>secondary cloud service providers</u> as part of its own <u>cloud services</u> [SOURCE: From ISO/IEC 22123-1:2021(en), 3.12.2]
procedure	specified way to carry out an <u>activity</u> or a <u>process</u> Note 1 to entry: Procedures can be documented or not. [SOURCE: ISO 9000:2000, 3.4.5]
process	set of interrelated or interacting <u>activities</u> which transforms inputs into <u>outputs</u> [SOURCE: From ISO Supplement:3.12]
product	output of an organization that can be produced without any transaction taking place between the organization and the customer

Term	Definition
	[SOURCE: ISO 9000:2000, 3.4.2]
production environment	The environment that serves customers
records system	information system which captures, manages and provides access (3.1) to records over time 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. [SOURCE: From ISO15489-1:2016]
recovery point objective RPO	point in time to which data are to be recovered after a <u>disruption</u> has occurred [SOURCE: From ISO/IEC 27002:2022(en), 3.1.29]
recovery time objective RTO	period of time within which minimum levels of <u>services</u> and/or products and the supporting systems, applications, or functions are to be recovered after a <u>disruption</u> has occurred [SOURCE: From ISO/IEC 27002:2022(en), 3.1.30]
reperformance	The auditor's independent execution of <u>procedures</u> or <u>controls</u> that were originally performed as part of the customer's internal controls [SOURCE: From IAASB Handbook of International Quality Control, auditing, Review, other Assurance and Related Service Pronouncements, 2017 Edition, Glossary of Terms]
requirement	need or expectation that is stated, generally implied or obligatory 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. Note 2 to entry: A <u>specified requirement</u> is one that is stated, for example in documented information. Note 3 to entry: A qualifier can be used to denote a specific type of <u>requirement</u> , e.g. product requirement, service requirement, customer requirement. [SOURCE: From ISO/IEC 27000:2018(en), 3.56]
residual risk	<u>risk</u> remaining after <u>risk</u> treatment Note 1 to entry: <u>Residual risk</u> can contain unidentified <u>risk</u> . Note 2 to entry: <u>Residual risk</u> can also be known as "retained <u>risk</u> ". [SOURCE: From ISO Guide73:2009(en), 3.8.1.6]
resource pooling	aggregation of a <u>cloud service provider's</u> physical or virtual resources to serve one or more cloud service customers [SOURCE: From ISO/IEC 22123-1:2021(en), 3.5.5]
restoration	reinstatement of the full or partial statement of <u>conformity</u> [SOURCE: From ISO/IEC 17000:2020(en), 8.5]
review	<subject matter> activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives [SOURCE: From ISO Guide 73:2009, 3.8.2.2]
review	<certification> consideration of the suitability, adequacy and effectiveness of <u>selection and determination activities</u> , and the results of these activities, with regard to fulfilment of <u>specified requirements</u> by an object of <u>conformity assessment</u> [SOURCE: From ISO/IEC 17000:2020(en), 7.1]
review report	the document written by the <u>CAR</u> after performing the <u>review</u> of the <u>evaluation</u> performed by the <u>audit team</u>

Term	Definition
risk	<p>effect of uncertainty on <u>objectives</u></p> <p>Note 1 to entry: An effect is a deviation from the expected — positive and/or negative.</p> <p>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, <u>product</u> and <u>process</u>).</p> <p>Note 3 to entry: Risk is often characterized by reference to potential events and consequences, or a combination of these.</p> <p>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.</p> <p>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.</p> <p>[SOURCE: From ISO Guide73:2009(en), 1.1]</p>
risk analysis	<p><u>process</u> to comprehend the nature of <u>risk</u> and to determine the level of <u>risk</u></p> <p>Note 1 to entry: Risk analysis provides the basis for <u>risk evaluation</u> and decisions about <u>risk</u> treatment.</p> <p>Note 2 to entry: Risk analysis includes risk estimation.</p> <p>[SOURCE: From ISO Guide73:2009(en), 3.6.1]</p>
risk assessment	<p>overall <u>process</u> of risk identification, risk analysis and <u>risk evaluation</u></p> <p>[SOURCE: From ISO Guide73:2009(en), 3.4.1]</p>
risk evaluation	<p><u>process</u> of comparing the results of risk analysis with <u>risk criteria</u> to determine whether the <u>risk</u> and/or its magnitude is acceptable or tolerable</p> <p>Note 1 to entry: Risk evaluation assists in the decision about <u>risk</u> treatment.</p> <p>[SOURCE: From ISO Guide73:2009(en), 3.7.1]</p>
risk identification	<p><u>process</u> of finding, recognizing and describing <u>risks</u></p> <p>Note 1 to entry: Risk identification involves the identification of <u>risk</u> sources, events, their causes and their potential consequences.</p> <p>Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.</p> <p>[SOURCE: From ISO Guide73:2009(en), 3.5.1]</p>
risk management	<p>coordinated <u>activities</u> to direct and control an organization with regard to <u>risk</u></p> <p>[SOURCE: From ISO Guide73:2009(en), 2.1]</p>
risk of material misstatement	<p>The risk that the subject matter information is materially misstated prior to the start of the engagement</p> <p>[SOURCE: From ISAE3000: 12.w]</p>
risk owner	<p>person or entity with the accountability and authority to manage a <u>risk</u></p> <p>[SOURCE: From ISO Guide73:2009(en), 3.5.1.5]</p>
risk treatment	<p><u>process</u> to modify <u>risk</u> (1.1)</p> <p>Note 1 to entry: Risk treatment can involve:</p> <ul style="list-style-type: none"> • avoiding the <u>risk</u> by deciding not to start or continue with the <u>activity</u> that gives rise to the risk; • taking or increasing risk in order to pursue an opportunity; • removing the risk source; • changing the likelihood; • changing the consequences; • sharing the <u>risk</u> with another party or parties [including contracts and <u>risk</u> financing]; and • retaining the <u>risk</u> by informed decision. <p>Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".</p>

Term	Definition
	Note 3 to entry: Risk treatment can create new risks or modify existing risks. [SOURCE: From ISO Guide73:2009(en), 3.8.1]
role	set of activities that serves a common purpose [SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.11]
role-based access control RBAC	security technique for authentication that authorizes operations or allows access to resources based upon the user's identity and his/her relationship to other users and entities EXAMPLE 1: A teacher has read/write access to the grades for his/her students (role: "the teacher of the student"), but no access to other students' grades EXAMPLE 2: A principal has read-only access to the grades of all of his/her teachers' students (role: "the principal of the teachers of the students"), but the principal is not permitted to change any grades [SOURCE: From ISO/IEC 20944-1:2013(en), 3.21.20.2]
sampling	selection and/or collection of material or data regarding an object of conformity assessment Note 1 to entry: Selection can be on the basis of a procedure, an automated system, professional judgement etc. Note 2 to entry: Selection and collection can be performed by the same or different persons or organizations. [SOURCE: From ISO/IEC 17000:2020(en), 6.1]
scope of certification	identification of — the service(s) for which the certification is granted, — the applicable certification scheme and scheme options, and — the standard(s) and other normative document(s), including their date of publication, to which it is judged that the service(s) comply Note to entry: The definition has been altered to include "scheme options", which may in the context of the EUCS cover in particular the selected evaluation level and extension profiles. [SOURCE: Adapted from ISO/IEC 17065:2012(en), 3.10]
secondary cloud service	cloud service of one cloud service provider which is used as part of a cloud service of one or more other cloud service providers NOTE: In ISO/IEC 22123-1, the term used is peer cloud service, which may lead to confusion in the context of the EUCSA. [SOURCE: From ISO/IEC 22123-1:2021(en), 3.12.2]
secondary cloud service provider	cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services [SOURCE: From ISO/IEC 22123-1:2021(en), 3.4.9]
security area	an area delimited by security perimeters, within which access is not controlled
security assurance	grounds for justified confidence that a claim about meeting security objectives has been or will be achieved [SOURCE: From ISO/IEC/IEEE 15026-1(2019):3.4]
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]
security perimeter	the physical border surrounding locations hosting CSP equipment and personnel, for which access is controlled

Term	Definition
security problem	statement which in a formal manner defines the nature and scope of the security that the object of conformity assessment is intended to address Note 1 to entry: This statement consists of a combination of: — threats to be countered by the object of conformity assessment, — the OSPs enforced by the object of conformity assessment, and — the assumptions that are upheld for the object of conformity assessment and its operational environment. [SOURCE: Adapted from ISO/IEC 15408-1:2009(en), 3.1.61]
security zone	area of a network in which limited data exchange with areas outside is allowed [SOURCE: From ISO/TR 11636:2009(en), 2.13]
selection	planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function Note 1 to entry: Selection activities vary widely in number and complexity. In some instances, very little selection activity may be needed. [SOURCE: From ISO/IEC 17000:2020(en), A.2.1]
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]
service provider external service provider	organization or an individual that enters into agreement with the CSP for the supply of a service [SOURCE: Adapted from ISO/IEC 27036:1-2014, 3.9]
service requirement	requirement that relates directly to a service, specified in standards or in other normative documents identified by the certification scheme Note 1 to entry: Service requirements are in the EUCS identified primarily in Annex A of the scheme. [SOURCE: Adapted from ISO/IEC 17065:2012(en), 3.8]
specified requirement	need or expectation that is stated Note 1 to entry: Specified requirements may be stated in normative documents such as regulations, standards and technical specifications. Note 2 to entry: Specified requirements can be detailed or general 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). [SOURCE: From ISO/IEC 17000:2020(en), 5.1]
Stakeholder Cybersecurity Certification Group SCCG	Advisory group composed of members selected from among recognised experts representing the relevant stakeholders [SOURCE: Adapted from Cybersecurity Act , Article 22]
state-of-the-art	developed stage of technical capability at a given time as regards products , processes and services , based on the relevant consolidated findings of science, technology and experience Note 1 to entry: The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the “generally acknowledged state of the art”. [SOURCE: From ISO/IEC Guide 63:2019, 3.18]
strategy	planned activities to achieve a long term or overall objective [SOURCE: ISO 9000:2015, 3.5.12]

Term	Definition
strong	not easily defeated, having strength or power greater than average or expected, able to withstand attack or solidly built [SOURCE: From ISO/IEC 19790:2012, 3.123]
subservice	service provided by a subservice provider
subservice provider subservice organization	third-party providing services to the CSP that contribute to the provision of the cloud service by the CSP NOTE: In particular, a secondary cloud service provider is a subservice provider to any primary cloud service provider that uses its services
subsystem	a set of elements, which is a system itself, and a component of a larger system [SOURCE: Wikipedia]
sufficiency of evidence	The measure of the quantity of evidence [SOURCE: From ISAE3000: 12.i.i]
supplementary cybersecurity information	Information related to cybersecurity to be made publicly available by any 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 NOTE: The information includes guidance and recommendations, the period during which security support will be offered, contact information for receiving vulnerability information and a reference to online repositories listing vulnerabilities. [From Cybersecurity Act, Article 55]
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]
support	set of activities necessary to ensure that an operational system or component fulfills its original requirements and any subsequent modifications to those requirements. NOTE: Examples include software or hardware maintenance, user training. [SOURCE: From ISO/IEC/IEEE 24756:2017, 3.4054]
surveillance	systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity 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. [SOURCE: From ISO/IEC 17000:2020(en), 8.1]
suspension	temporary restriction of the statement of conformity by the body that issued the statement, for all or part of the specified scope of attestation [SOURCE: From ISO/IEC 17000:2020(en), 8.2]
system	a group of interacting or interrelated entities that form a unified whole [SOURCE: Wikipedia]
system component	a functional component 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 NOTE: system components may include software, hardware, or both. EXAMPLES: firewalls, load balancers, web servers, application servers, database servers.

Term	Definition
	[Source: Adapted from C5:2020]
technical expert	person who provides specific knowledge or expertise to the audit team [SOURCE: From ISO/IEC 17021-1:2015(en), 3.14]
tenant	one or more cloud service users sharing access to a set of physical and virtual resources [SOURCE: From ISO/IEC 22123-1:2021(en), 3.5.2]
test environment	The environment in which new and changed code is exercised via automated or non-automated techniques
test	activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component [SOURCE: IEEE Std 610.12-1990]
testing	determination of one or more characteristics of an object of conformity assessment , according to a procedure 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. Note 2 to entry: The results of testing can be expressed in terms of specified units or objective comparison with agreed references. 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 . [SOURCE: From ISO/IEC 17000:2020(en), 6.2]
third-party	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 [SOURCE: From ISO/IEC 17000:2020(en), 2.2]
third-party conformity assessment activity	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 [SOURCE: From ISO/IEC 17000:2020(en), 4.5]
threat	potential cause of an unwanted incident, which can result in harm to a system or organization [SOURCE: From ISO/IEC 27000:2018, 3.74]
top management	person or group of people who directs and controls an organization at the highest level Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization. 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. [SOURCE: ISO Supplement:3.5]
trust service	an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services [SOURCE: From Regulation (EU) No 910/2014, Article 3(16)]
trust service provider	a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider [SOURCE: From Regulation (EU) No 910/2014, Article 3(19)]

Term	Definition
tunnel	data path between networked devices which is established across an existing network infrastructure Note 1 to entry: Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits [SOURCE: From ISO/IEC 27033-1:2015(en), 3.40]
undertaking	entities engaged in an economic activity, regardless of their legal status and the way in which they are financed including all linked enterprises or connected undertakings that form a group through the direct or indirect control of an enterprise or undertaking by another. [SOURCE: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Article 2(27)]
validation	confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements (5.1) have been fulfilled Note 1 to entry: Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use. [SOURCE: From ISO/IEC 17000:2020(en), 6.5]
verification	confirmation of truthfulness through the provision of objective evidence that specified requirements (5.1) have been fulfilled 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. [SOURCE: From ISO/IEC 17000:2020(en), 6.6]
version control	establishment and maintenance of baselines and the identification and control of changes to baselines that make it possible to return to the previous baseline [SOURCE: From ISO/IEC/IEEE 24765:2017(en), 3.4546]
virtual local area network VLAN	independent network created from a logical point of view within a physical network [SOURCE: From ISO/IEC 27033-1:2015(en), 3.41]
vulnerability	weakness of an asset or control that can be exploited by one or more threats [SOURCE: From ISO/IEC 27000:2018(en), 2018, 3.77]
withdrawal cancellation	revocation of the statement of conformity by the body that issued the statement [SOURCE: From ISO/IEC 17000:2020(en), 8.3]

K.3 DERIVED TERMS

Some terms used in the candidate scheme, its annexes and its requirements are derived from some of the terms defined above, typically by changing the grammatical nature of the word (e.g., deriving a verb or an adjective from a noun). The most commonly derived terms are listed below, and their use should be understood as referring to the definition of the term that they are derived from.

Term	Derived term	Definition
accreditation	accredited (adj.)	of a CAB that has gone through accreditation NOTE 1: the use of "accredited" usually implies that the accreditation is currently valid

Term	Derived term	Definition
appropriateness of evidence	appropriate evidence	evidence for which appropriateness is there
approve	approval	the action to approve
audit	to audit (v.)	to perform an audit
authorisation	authorised (adj.)	to have obtained an authorisation, for a CAB
authorisation	to authorise (v.)	to perform the authorisation of a CAB
certification	certificate (n.)	attestation document issued by an independent third-party certification body
certification	certified (adj.)	of a product, service or process that has gone through certification NOTE 1: the use of "certified" usually implies that the certification is currently valid NOTE 2: throughout the document, the locution "certified cloud service" is intended to mean "a cloud service certified in the EUCS scheme", unless otherwise specified
certification	to certify (v.) to issue a certificate	to perform a certification activity
certification	certificate issuance	attestation activity by an independent third-party certification body
evaluation	evaluated (adj.)	undergoing an evaluation
evaluation	to evaluate (v.)	to perform an evaluation
expiry	expired (adj.)	of a statement of conformity that has reached its expiry
expiry	expire (v.)	to reach its expiry
inquiry	inquire (v.)	to perform an inquiry
inspection	inspect (v.)	to perform an inspection
monitoring	monitored (adj.)	of a system, process or activity under monitoring
monitoring	to monitor (v.)	to perform monitoring
requirement	security requirement	requirement on a security control
review	to review (v.)	to perform a review NOTE: There are two different meanings of review, in different contexts, and the verb can apply to both nouns
sufficiency of evidence	sufficient evidence	evidence for which sufficiency is appropriate
suspension	suspended (adj.)	of a certificate after its suspension and before its withdrawal or restoration
suspension	to suspend (adj.)	to perform a suspension
withdrawal	withdrawn (adj.)	of a certificate after its withdrawal

Term	Derived term	Definition
withdrawal	to withdraw (v.)	to perform a <u>withdrawal</u>

K.4 REQUIREMENT TERMS

There are a few terms (in particular verbs) that are used in the definition of requirements, as follows. It is not clear how these terms should be included in the overall terminology:

Term	Definition
approve	<any document or information> the action by an authorized body to confirm that a document conforms to <u>requirements</u> or expectations
communicate	<any document or information> the action of sharing the document or information with targeted persons through an explicit action (email, posters, etc.) NOTE: For policies and procedures, this term is only used in ISP-02 and where specific and requirements specify a specific form of communication (typically, to additional parties)
describe	provide specific details of an entity [SOURCE: ISO/IEC 15408-1:2009(en), 3.1.21]
define	<policies and procedures> to perform the actions described in ISP-02 for the definition of a procedure (document it, communicate it, have it approved, etc...)
document	<policies and procedures> the actions of designing policies and procedures related to a given topic or <u>process</u> and of preparing documentation targeting the relevant stakeholders NOTE: This term is only used in ISP-02 and where specific and requirements specify a specific form of documentation
implement establish?	<policies and procedures> the action of putting the policies and <u>procedures</u> into practice NOTE: C5 does not explicitly refer to implementation.
maintain	<any document> the continuous action of keeping a document up-to-date
make available	<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 NOTE: This term is only used in ISP-02 and where specific and requirements specify a specific form of distribution (typically, to additional parties)
monitor	
review	<any document> the action of comparing the document with up-to-date information and modifying it if needed
specify	provide specific details about an entity in a rigorous and precise manner [SOURCE: ISO/IEC 15408-1:2009(en), 3.1.66]

In addition, some of the terms used in the requirements on controls lack a proper definition:

Term	Definition
mechanism, measure, safeguard	The idea of safeguard is interesting (apparently used mostly in HIPAA, but adopted by C5), but we should consider selecting or differentiating between mechanism, measure and safeguard.
technical safeguard	
organizational safeguard	
database, knowledge repository, list, catalogue, inventory	collection of machine-readable information organized so that it can be easily accessed, managed and updated [SOURCE: ISO 5127:2017, 3.1.13.03]

POLITICO



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