CSPCERT WG
(Milestone 3)
Recommendations for the implementation of the CSP Certification scheme

Final Editor:	Borja Larrumbide Martinez and Leire Orue-Echevarria
Status-Version:	Final
Date:	07.06.2019
Distribution level (CO, PU):	Public

Author(s)	Aurelien Leteinturier; Borja Larrumbide; Bert Tuinsma; Clemens Doubrava; Daniele Catteddu; Hans Graux; Leire Orue-Echevarria; Thomas Niessen; Tom Vreeburg; William Ochs
Contributor(s)	Andreas Fuchsberger; Francois-Xavier Vincent; Hem Pant; James Mulhern, Jesus Luna; Saurabh Ghelani; Volkmar Lotz
CSPCERT WG Co-chairs	Borja Larrumbide (BBVA), Helmut Fallmann (Fabasoft)
Approved	All drafting members

Abstract:	This document presents the recommendations of the CSPCERT Working Group towards the implementation of a European wide Cloud Certification Scheme in the context of the Cybersecurity Act
Keyword List:	Cybersecurity act, cloud security certification scheme, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISAE 3402, ANSSI SecNumCloud, BSI C5, EUCA, ENISA, assurance levels.
Disclaimer	This document reflects only the authors' views and the Commission is not responsible for any use that may be made of the information contained therein

Table of Contents

List of Tables

List of Figures

Terms and abbreviations

ANSSI	Agence nationale de la sécurité des systèmes d'information
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Controls Catalogue
CAB	Conformity Assessment Body
CAM	Conformity Assessment Methods
CB	Conformity Body
CCAL	Cloud Computing Assurance Level
CCSM	Cloud Computing Schemes Metaframework
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CSAR	Cybersecurity Act Requirements
CSPCERT	Cloud Service Provider Certification group
CVE	Common Vulnerabilities and Exposures
EC	European Commission
ECCG	European Cybersecurity Certification Group
EU	European Union
EUCA	European Union Cybersecurity Act
HSM	Hardware security module
ISAE	International Standard on Assurance Engagements
ISMS	Information security management system
ISO	International Standardization Organization
NAB	National Accreditation Body
NCCA	National Cybersecurity Certification Authority
PII	Personal Identifiable Information
SGOV	Scheme Governance
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WG	Working Group
WTO	World Trade Organization

The abbreviations, CCAL, CSAR and SGOV are used to as a prefix to section 3, 4 and 5 respectively.

Executive Summary

This document presents the work performed by the Cloud Service Provider Certification Working group (from now on, CSPCERT WG), created on December 2017, from April 2018 to June 2019 in response to the European Cybersecurity Act (EUCA), Title III, which aims to set the grounds to establish an EU-wide framework for cybersecurity certification of ICT services, products and processes, including those services provisioned by Cloud Service Providers (CSP).

The objective of the CSPCERT WG is to explore the possibility of developing a European wide Cloud Certification Scheme in the context of the Cybersecurity Act and to provide the European Commission and ENISA with a set of recommendations that should be taken into consideration when implementing the cloud certification scheme.

The work of the CSPCERT WG has revolved around three distinct milestones: (1) Milestone 1, focused on the elaboration of the security objectives that an EU-wide certification scheme shall include. These security objectives are based on the analysis of existing standards, schemes and good practices. This milestone also includes the definition of a methodology to incorporate additional security objectives that may come up in the future. The document resulting from this milestone can be found in Annex 1. (2) Milestone 2 focused on a comparative analysis of the most relevant conformity assessment methodologies, their approaches and distinct elements. The result of this milestone can be found in Annex 2. (3) Milestone 3, this document, which elaborates upon the previous documents, the results of the open consultation held during January – February 2019 and provides additional and new content in the form of recommendations for the European Commission and ENISA.

As a general recommendation, the CSPCERT WG proposes the Commission to (1) include the development of an EU-wide cloud security certification scheme in the Union rolling work programme for European cybersecurity certification under the Cybersecurity Act, and (2) to request ENISA to prepare a candidate scheme on the basis of the present proposal, as part of the execution of that Union rolling work programme. The outcome of the CSPCERT WG to the European Commission is not proposing a completely new certification scheme but providing guidance for a scheme based on existing practices/schemes/standards used by the industry and internationally recognized.

A suitable certification scheme is one that meets the specifications in the text of the European Cybersecurity Act. ENISA should assess the adherence to those specifications based on transparent evaluation criteria. In this paper the CSPCERT WG presents recommendations for a cloud certification scheme. The recommendations have been divided into three categories:

1. Recommendations related to Cloud Computing Assurance Levels (CCAL), section 3, which include recommendations pertaining to the CSP service certification scheme objectives and assurance levels;
2. Recommendations related to Cybersecurity Act Requirements (CSAR), section 4, which present recommendations refining the elements and additional information that the certification should present;
3. Recommendations related to the Scheme Governance (SGOV), section 5, which include recommendations pertaining to the governance of the CSP service certification scheme.

1. Recommendations related to Cloud Computing Assurance Levels (CCAL)

Assurance levels

As permitted by the European Cybersecurity Act, the EU-wide cloud security certification scheme should feature three assurance levels: 'basic', 'substantial' and 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of ICT products, ICT service or ICT process, in terms of the probability and impact of an incident. It is important that ENISA provides a clear guidance on how to perform this risk assessment and link the assurance level to the cloud service. For the cloud computing certification scheme this guidance should include, at least, a) a tailored description of what the basic/substantial/high assurance level indicates, and b) examples of which level of assurance should be associated with which service. Finally, the certification program should allow a cloud service provider to bundle services into a single certification, as long as those are transparently included into the original or subsequent audit cycles and that they meet the required assurance for that certification level.

Evaluation criteria

The CSPCERT WG has developed a set of high level and detailed security objectives based upon two studies created by ENISA [1] and the European Commission [2]. This set of security objectives was created as part of Milestone 1 and was subject to public consultation in January/February 2019. It is included in Annex 1 to this paper. This set of evaluation criteria should make it possible to create a taxonomy of security domains that could map existing international standards and certifications such as SecNumCloud from ANSSI [3], C5 from BSI [4], ISO/IEC 27002 [5], ISO/IEC 27017 [6], and ISO 27018 [7]. Underlying certification frameworks and standards were also considered, such as, CSA Cloud Control Matrix [8] and NIST SP 800-53 [9]. The CSPCERT WG recommends having an EU taxonomy like the one presented in Annex 1 in order to remain flexible for future updates, modifications or additions of new or existing international standards and certifications. For this reason, a methodology such as the one used in Milestone 1 should be used based on governance and procedures. which should be defined in detail by ENISA.

Conformity assessment

The CSPCERT WG proposes three different conformity assessment methodologies: Evidence Based Conformity Assessment and two Third-Party Conformity Assessments (ISO- and assurance-based) resulting in the issuance of a European Certificate. These conformity assessment methodologies align with the ones currently used in auditing and certification standards. These conformity assessment methodologies were selected from a list of methodologies currently in use by providers of cloud services. The underlying analysis was part of Milestone 2 which was also subject to public consultation in January/February 2019. For a more detailed description of these methodologies please refer to Annex 2.

An important objective of a recognized conformity assessment methodology is to reduce the level of bias and make sure that the level of trust provided by the conformity assessment bodies and the individual auditors is within acceptable ranges everywhere. ENISA, together with the National Cybersecurity Certification Authorities and the National Accreditation Bodies, should assess third-party conformity assessment methodologies for safeguards regarding the level of trust provided prior to an accredited use of the methodology.

Each conformity assessment methodology reviewed in this document includes a systematic way (namely, procedures) to assess the compliance of a cloud service to a set of criteria. As both the

procedures (according to Article 52 of the EUCA) and the criteria may differ between the assurance levels 'basic', 'substantial', and 'high', the certification scheme should provide clear guidance on the required procedures and criteria per assurance level.

For the effectiveness of the certification, the cloud service, including the subservices used by the CSP in the cloud computing supply chain, should be included in the scope of the certificate. The composition of the service in its subservices and subservice providers should be disclosed.

For High and Substantial offers, with the unique threat landscape of cloud services, it is recommended that an annual audit of cloud services is a minimal requirement. In addition to that, for High level, it is recommended to adopt a continuous auditing approach in order to increase the frequency of the evaluations and to ensure a level of assurance that goes beyond a "point-in-time" or "over-a-period-of-time". Further, audits must measure operational effectiveness at these levels, and not merely control existence. For Basic offers, an evidence-based conformity assessment certification should not exceed a 3-year cycle. ENISA should clarify what would trigger a new out-of-cycle review.

Finally, for High and Substantial, ENISA should consider future clarifications on the implementation and utilization of Continuous Monitoring. While Milestone 2 did not find that Continuous Monitoring had sufficiently developed during this working period, it is expected that this will mature and could be part of future requirements for Substantial and High.

2. Recommendations related to Cybersecurity Act Requirements (CSAR)

Article 51 of the European Cybersecurity Act establishes a set of security objectives that shall be fulfilled. For almost every objective, the CSPCERT WG has defined a recommendation or set of recommendations, listed in section 3.2 of this document. The recommendations related to the elements of the scheme are included in section 4.1.

To this end, the CSPCERT WG proposes a baseline certification that could optionally be enhanced with further regulatory requirements coming from regulators, supervisors or the industry such as future GDPR certifications, Outsourcing requirements from the European Banking Association (EBA), e-evidence, eIDAS, e-privacy or PCI-DSS to name a few examples. Moreover, CSPCERT WG also notes that CSPs shall retain the ability to provide services outside the scope for which they are being certified, but cannot, in this case, use this certification for the purpose of providing these services.

3. Recommendations related to the Scheme Governance (SGOV)

The CSPCERT WG recommends that ENISA is requested to establish governance requirements as a part of the scheme that enables to implement and maintain a cloud security certification throughout the EU in accordance with the EUCA. Apart from the bodies and regulations mentioned in the EUCA, the document at hand identifies a number of specific items of interest for cloud security certification and also identifies topics that, in the vision of the CSPCERT WG, need to be addressed in general since this will be the first certification scheme to be implemented. Some important high-level recommendations in this respect relate to:

- A suitable certification is a scheme that meets exactly and precisely all the specifications established according to the requirements of the EUCA.
- ENISA should assess the adherence to the specifications based on a transparent evaluation criteria.

- ENISA should involve all stakeholders including governments, regulators, supervisors, end user representatives, and the industry to provide further input on use cases, risk scenarios, and assurance levels, avoiding overlaps with other regulations and facilitating security, trust, privacy, transparency and free flow of data.
- ENISA should maintain a dedicated website with information on, and publicising, the cloud cybersecurity certification scheme, including applicable reference documentation, certificates and EU statements of conformity, withdrawal or expiration, as provided by the EUCA

1 Introduction

1.1 About this document

The European Union Cybersecurity Act (EUCA)[1] sets the ground to establish an EU framework for cybersecurity certification of IT services, products and processes, including those services provisioned by Cloud Service Providers (CSP). The Cloud Service Provider Certifications Working group (CSPCERT WG) was created on December 12th, 2017 to provide expert recommendations to the European Commission for a scheme on cybersecurity certification of cloud services.

The objective of the CSPCERT WG is to explore the possibility of developing a European Cloud Certification Scheme in the context of the European Cybersecurity Act (EUCA) and come up with a recommendation that will be presented to the European Commission and ENISA (European Union Agency for Network and Information Security). The following picture outlines the initial stage and composition of the CSPCERT WG and its governance documents.

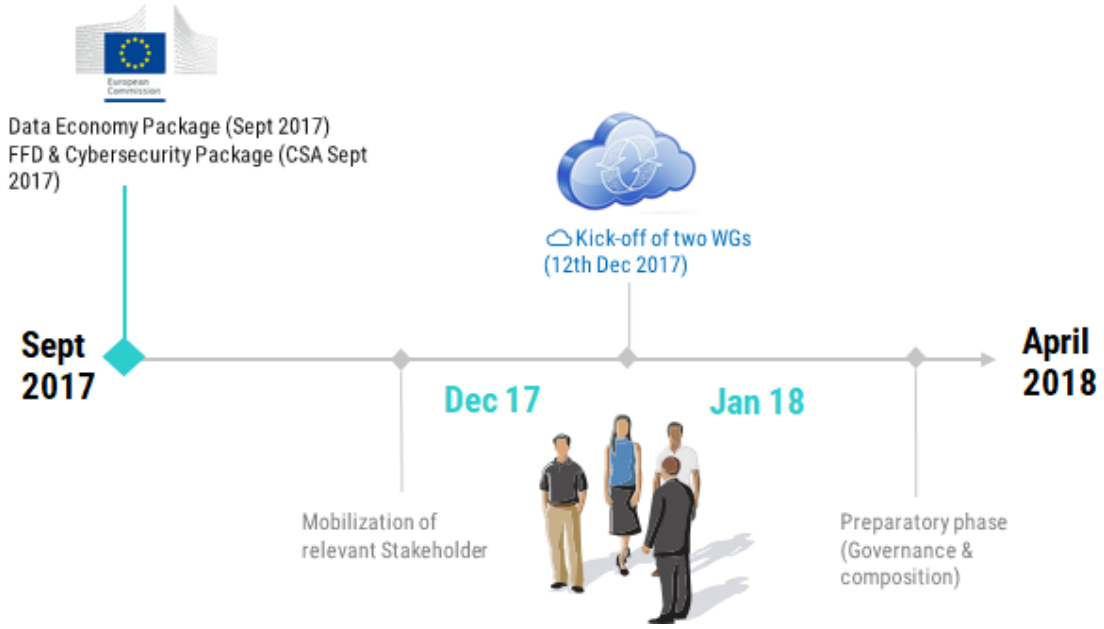

Figure 1. CSPCERT WG timeline

According to the European Cybersecurity Act, the European Commission can request ENISA to develop such a cybersecurity certification scheme. Therefore, the recommendations of the CSPCERT WG should be seen as a starting point for ENISA to further develop and create a final Cloud Service Provider Certification scheme.

The CSPCERT WG has two types of memberships: Drafting members which are the actual experts drafting the proposal and observer members which are experts that are not directly involved in the elaboration of the proposal but have full read access to all documents and minutes generated by the

[1] The latest version of the Cybersecurity Act available while drafting this document was : http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2019-0151#BKMD-20
The final version of the Cybersecurity Act was approved the same day this document was published and it can be found here: https://europa.eu/!bX86Fp

drafting members. The following graphic depicts the types of memberships as well as major requirements set in the rules of procedure and governance elaborated and approved by the drafting members and co-chairs.

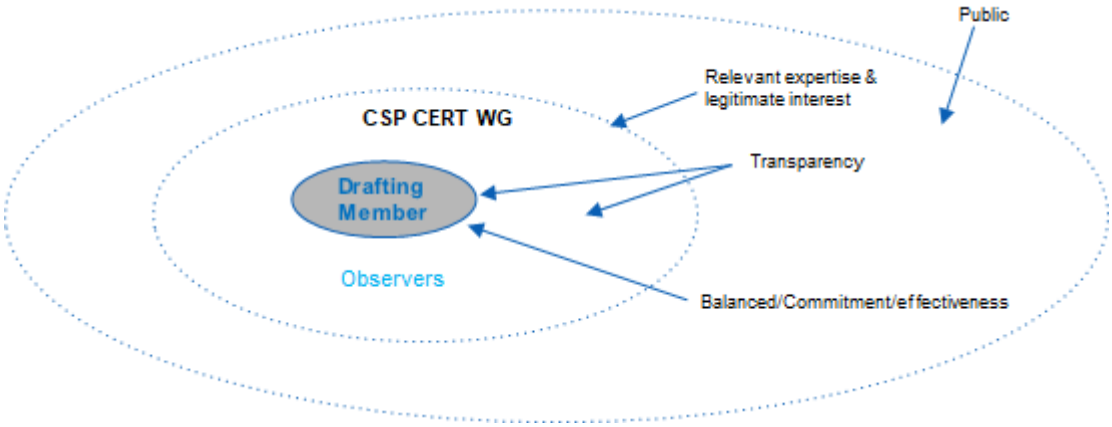

Figure 2. CSPCERT WG Types of members

The CSPCERT WG, composed of experts from the private and public sector, produced three deliverables (i.e., "Milestone" documents) and organized an Open Consultation to receive public feedback on the initial two Milestones.

Figure 3. CSPCERT WG Milestones and Open consultation dates

All joint documents created by the CSPCERT WG were then considered for the elaboration of a final document to be submitted to the European Commission and ENISA. The deliverables produced by CSPCERT WG are the following:

- Milestone 1 recommends a comprehensive set of security objectives, which (from the CSPCERT WG perspective) should be part of any EU-wide certification scheme aligned to the EUCA. The proposed set of security objectives is based on the analysis of existing standards and good practices. Milestone 1 also considers the need to have a methodology to update the security objectives with future ones.
- Milestone 2 provides a comparative analysis of the most relevant conformity assessment methodologies. This Milestone outlines the different approaches to assess conformity of a cloud service to a predefined set of cloud security requirements (e.g., those from Milestone 1) and describes the various elements of those approaches.

- Milestone 3 (this document) collects and integrates the feedback of the CSPCERT WG Open Consultation[2], and develops through the inputs provided by all drafting members of the CSPCERT WG into a final recommendation for the European Commission and ENISA which is the present document.

As a closing remark, it is important to mention that all deliverables produced by the CSPCERT WG are based on existing international standards and state of practice methodologies used by the industry and European Member States' cloud security certification schemes currently in force, at the time Milestone 1 started., For instance, SecNumCloud [10] [3] from ANSSI and C5 [4] from BSI met those criteria. The CSPCERT WG also took into account two studies created by the European Commission [2] and ENISA [1] which analysed existing private international cloud certifications and standards such as Cloud Security Alliance Cloud Control Matrix v3.0.1 [8], C5 [4], NIST SP 800-53 [11] and ISO/IEC 27000 [12] [12] [6] [7] series. The CSPCERT WG underlines that existing certifications and standards should be taken into consideration when creating an EU-wide cloud security certification.

The outcome of the CSPCERT WG to the European Commission is not about a completely new certification scheme, but towards providing guidance for such a scheme based on existing practices/schemes/standards used by the industry and internationally recognized.

1.2 Document structure

The rest of this document is structured as follows:

- The main body of the document, namely sections 2 - 5, lists the recommendations from the CSPCERT WG for the implementation of a Cloud Computing Service providers certification scheme;
- Annex 1 contains the security objectives elicited as well as the methodology followed and the resulting map analysis, achieved during Milestone 1;
- Annex 2 contains a description of conformity assessment methodologies, achieved during Milestone 2;
- Annex 3 contains the glossary covering the terms used in the EUCA and the one used in current standards specifications;
- Annex 4 includes a template proposal for a report.

[2] https://cspcerteurope.blogspot.com/2019/01/questionnaire-for-open-consultation-of.html

2 Setting up a certification scheme within the framework of the Cybersecurity Act

Title III of the EUCA contains the main rules and principles for defining certification schemes, in Articles 46 to 57. Each Article covers specific requirements and topics pertaining to the establishment and operation of a certification scheme.

The following sections of the document provides several detailed recommendations for the implementation of those requirements from Title III of the EUCA, in relation to the certification of services provided by a Cloud Service Provider. These have been subdivided into three categories, corresponding to the next three sections of the document:

1. **Cloud Computing Assurance Level (CCAL) recommendations**, i.e. recommendations pertaining to the CSP service certification scheme objectives and assurance levels;
2. **EU Cybersecurity Act Requirements (CSAR)**: i.e. recommendations refining the high-level requirements of the EUCA requirements pertaining to the CSP service certification scheme;
3. **Scheme Governance (SGOV) recommendations**, i.e. recommendations pertaining to the governance of the CSP service certification scheme

This document does not repeat any requirements of the EUCA which are sufficiently detailed in the Act itself, and that are common to all certification schemes. These aspects (for example, the decision-making procedure used to formally adopt the scheme) are not in the scope of the CSPCERT WG activities.

The matrix below maps each Article of Title III of the EUCA to the corresponding recommendations stated in the paragraphs of this part of this document:

Table 1. Correspondence between the articles of the EU Cybersecurity Act and this document

Articles	Content	CCAL	CSAR	SGOV
46, 47 and 48	General considerations regarding all cybersecurity certification frameworks			
49 and 50	Preparation, adoption and review of a European cybersecurity certification scheme, and publication of schemes and certificates on a centralized website		partly	
51	Security objectives of European certification schemes	X		
52 and 53	Assurance levels of European certification schemes, and conformity assessments	X		
54 and 55	Elements of European cybersecurity certification schemes and Cybersecurity information for certified products, process and services		X	
56	Cybersecurity certification, i.e. indicating who is able to deliver certificates regarding a specific assurance level		X	
57	Impact on national cybersecurity certification schemes and certificates, describing legal implications and transition rules between legacy national schemes and			X

Articles	Content	CCAL	CSAR	SGOV
	corresponding European certification schemes after their adoption			
58 and 59	National cybersecurity certification authorities (NCCA), which describes roles and duties for the NCCA in Article 58. Article 59 covers the peer review mechanism, which will be used between and in relation to national cybersecurity certification authorities	X		X
60 and 61	Conformity assessment bodies and their notification to the European Commission in relation to specific schemes			X
62	Role of the European Cybersecurity Certification Group			X
63, 64 and 65	Complaints handling, effective judicial remedy and penalties regarding a conformity assessment body or a certificate		X	X

3 CCAL Objectives and Assurance levels for the CSP Certification

3.1 Scope of the Certification

In order to be certified, the cloud service must meet all the requirements of the certification scheme reference document that are applicable to the service boundary (e.g. SaaS, PaaS, IaaS, XaaS) and the chosen level of assurance.

3.2 Refined objectives for the European CSP Service Certification

The objectives for a certification scheme are described in Article 51 of the EUCA. The assessment of the correct implementation of the controls that achieve the security objectives listed in the Milestone 1 document (see Annex 1) with a methodology from the ones listed in the Milestone 2 document (see Annex 2) should be a guide to ensure that all these objectives are fulfilled regarding a certain assurance level.

The EUCA helps to define a set of principles from which security governance of cloud computing services can be achieved throughout the European Union. Cloud computing is seen as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Considering the nature of cloud computing services, these objectives as described in the EUCA, require further information. We have made some recommendations to avoid misunderstanding and missing important objectives for the CSP Service Certification scheme.

The following paragraphs shown in italics are the verbatim of Article 51 of the EUCA, broken down into bullet points from A to J. Each recommendation made by the CSPCERT WG is included in a grey cell table.

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 lifecycle 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 lifecycle of the ICT product, ICT service or ICT process;

(c) that authorised persons, programs or machines are able to only access the data, services or functions to which their access rights refer;

REC1: ENISA should include, as a set of security objectives, those security objectives defined in Milestone 1 document located in Annex 1 (e.g. section 3.4 'identity and access management' and section 3.5 'cryptography and key management') and extend them not only to include people but also programmes, machines, APIs and associated technology.

Justification: The security objectives located in the Milestone 1 document present the methodology followed by the CSPCERT WG, and it enumerates the set of security objectives created via a high-level gap analysis which took into account the following schemes: ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5, and the ENISA Metaframework schemes for the cloud. This Annex 1 was released as a stand-alone document and made available to a public consultation during January and February of 2019. The CSPCERT WG agreed to incorporate into the final proposal several comments and considerations received.

(d) to identify and document known dependencies and vulnerabilities;

REC2: Products and services should be updated at a time pace directly proportional to the risk associated with the known vulnerability and sensitivity level of the offering, in order to ensure a constant level of security regarding said discovered vulnerabilities. CSPs should demonstrate an active vulnerability management program (see Annex 1, section 3.7. OS.7 in 'Operational Security'), which incorporates rapid remediation that is commensurate with the assurance level of their certification.

Justification: An active vulnerability management program is a recognized hallmark of a secure cloud offering. Components of a strong vulnerability management program should include evidence that the CSP is maintaining (for a new certification) or has maintained (for renewal certifications) the stated security level of the environment. Components could include evidence requirements of tracking weaknesses identified, resolution of said weaknesses, patch management, configuration management, timely notification to customers, etc. REC3, would be expected to be more rigorous based upon the sensitivity level of the offering or certification level - basic, substantial, or high.

REC3: ENISA should establish guidelines on if/when/how a security incident affecting the certified service should trigger a re-assessment.

Justification: Clear guidance is needed, classified by assurance level, on when a security incident should trigger any ex post investigative review of a CSP certified service outside of their normal audit cycle.

REC4: ENISA, should establish guidelines for a continuous auditing process for certified offerings, which would be proportionate with the CCAL of the offer.

Justification: Clear guidance on the audit cycle of any certification is foundational to any certification framework. This must be established, for each of the assurance levels.

(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;

REC5: ENISA should consider including as a set of minimum security objectives, as those already defined in Milestone 1 document which can be located in Annex 1 (e.g. section 3.7 'Operational security' and more specifically OS.6).

Justification: The CSP CERT WG conducted during milestone 1 a study based on several studies, standards and certifications, and proposed a set of minimum Security Objectives.

(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

REC6: ENISA should consider including as a set of minimum Security Objectives that help ensure security-by-design such as those already defined in Milestone 1 document (e.g. section 3.15 'Systems security and integrity').

Justification: The Security Objectives have already been defined during milestone 1 which is considered as the minimum baseline ensures compliance with this requirement.

(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;

REC7: ENISA should consider the set of Milestone 1 Security Objectives that are already defined in Milestone 1 document and presented in Annex 1 (e.g. section 3.10 'Business continuity' and 3.11 'Incident management').

Justification: The Security Objectives have already been defined during milestone 1 which is considered as the minimum baseline ensures compliance with this requirement

(i) that ICT products, ICT services and ICT processes are secure by default and by design;

REC8: ENISA should consider including as a set of minimum Security Objectives those already defined in Milestone 1 document presented in Annex 1 (e.g. section 3.15 'Systems security and integrity').

Justification: The Security Objectives have already been defined during milestone 1 which is considered as the minimum baseline ensures compliance with this requirement.*(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.*

REC9: ENISA should consider including as a set of minimum Security Objectives those already defined in Milestone 1 document presented in Annex 1 (e.g. section 3.15 'Systems security and integrity' and section 3.7 'Operational security').

Justification: The Security Objectives have already been defined during milestone 1 which is considered as the minimum baseline ensures compliance with this requirement.

REC10: Certification schemes should include Cloud SLAs in certification processes. Such Cloud SLAs should be based on international standards (e.g. ISO/IEC 19086-4 [13]), so committed Security Objectives (please refer to Milestone 1 in Annex 1) are transparently communicated to the interested parties (e.g., Cloud Service Customer and business partners).

Justification: Usage of standardized Cloud SLAs will also benefit the CSP's objective assessment through auditing mechanisms. SLAs are a foundational aspect for a cloud offering that allows for monitoring of services, customer provisioning, quality of services, and even business continuity support.

3.3 Assurance levels

3.3.1 Risk management and assurance level

This section presents the recommendations of the CSPCERT WG with respect to Article 52 of the EUCA. The wording from the EUCA is expressed in italics. The text not in italics express the recommendations and rationale coming from the CSPCERT WG.

The first paragraph of the Article 52 stresses that certification schemes should consider different assurance levels by stating:

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.

A proper risk analysis would define the requirements of a particular level of certification taking into account the benefits versus cost, the risk level and the impact of a cyber incident on the cloud service. Any assurance level assigned to a qualified cloud service through the Cybersecurity Act certification scheme should conduct an internationally or industry recognized risk analysis, which should be reviewed as part of the final certification classification.

Risk is the effect of an uncertainty as to achieving a set of specific objectives. This is expressed in terms of a combination of consequences of an event and of its likelihood [14]: any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems.

Risk is based on two dimensions:

1. The likelihood or probability that an event will occur;
2. The degree or magnitude of impact if the event occurs.

Performing a proper risk analysis requires that both dimensions need to be considered and assessed. Based on the outcome of the risk assessment, a required level of assurance can be determined.

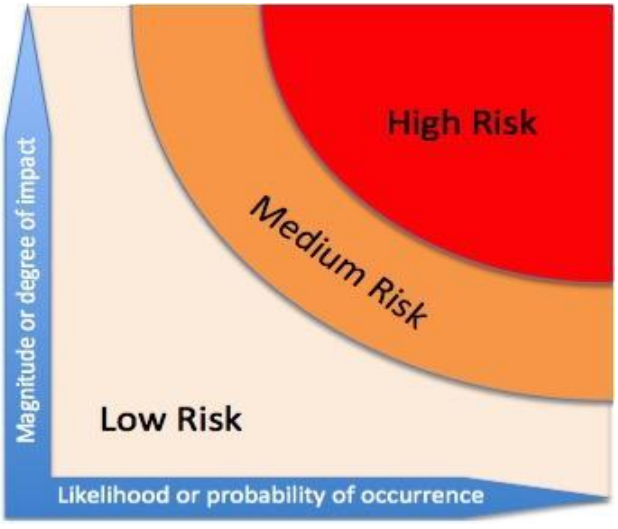

Figure 4. Dimensions of a risk

There are three areas which can be impacted by recognised risks:

- Personal: when the compromise of a product, system or service reaches the material, moral or psychological security of an individual;
- Business (Economical/ Reputational): when a compromised product, system or service influences the reliability of financial data and/or personal data, thus reaches the material security of an enterprise
- Societal: when the compromised product, system or service impacts the security of the population or the societal consistency;

Even, if it is difficult to foresee all the intended usage of cloud services on a long or even mid-term, it is still possible to consider some tendencies. Thus, it is possible to foresee different levels of certification required for various kinds of applications, according to the impact of a malicious event that could disrupt it.

The assurance levels as defined in the EUCA in the Article 52 regarding the potential of the attacker and the conformity of the state-of-the-art, respectively, are as follows:

- Basic: "*a level which aims to minimise the known basic risks for cyber incidents and cyber-attacks.*"
- Substantial: "*a level which aims to minimise known cyber risks, cyber incidents and cyber-attacks carried out by actors with limited skills and resources.*"
- High: "*level which aims to minimise the risk of state-of-the-art cyber-attacks carried out by actors with significant skills and resources*"

REC11: Cyber-attacks and Cyber Incidents are not the only source of disruption (intentional). The CSP service certification should also take into account operational disruptions, which can be unintentional.

Justification: The EUCA specifically mentions potential attacks and risks to a system for each of the levels, namely, basic, substantial, and high. The CSPCERT WG would like highlight that there is no coverage in the EUCA for operational or unintentional disruptions of a service and so it recommends including it in the final scheme as it foresees issues arising from change management, lack of testing, etc...

REC12: The definitions of the assurance levels basic/substantial/high in the EUCA do not provide a sufficiently clear guidance on which assurance level should be associated to which potential Personal/Business/Societal risk scenario impacts.

For the cloud computing certification scheme the CSP CERT WG recommend that ENISA should provide: a) a tailored description of what the basic/substantial/high assurance level indicates, and 2) examples of which level of assurance should be associated to which services (Table 2 provides some initial examples)

Justification: Public adoption, CSP utilization, and certification authorities will need a measurement by which to determine whether an attested CSP service aligns to an appropriate assurance level taking into account potential risk scenario impacts. CSPCERT WG has provided examples of what some of

these may look like in the final scheme for ENISA. ENISA should provide a final table as part of their implementation, which should mature over time with evolving threat landscapes and risk scenarios.

REC13: ENISA, for the purposes of a consistent approach across the EU, should establish as part of this recommended scheme, accompanying guidelines on appropriate certification and/or assurance levels for particular use cases. At the very least, it is recommended that this should be quantified by ENISA for the public sector, critical and essential operators.

Further, under any Cloud Shared Responsibility Model, the ability of a Cloud service to minimise the risk of a cyber incident relies on how the cloud service is used and configured. Thus, the certification scheme should encourage CSPs to provide guidance on how customers should secure their use of cloud.

Justification: To increase adoption rates and certification utilization, a clear guidance, which can mature over time, should be presented to the public, addressing how to select a cloud service in relation to choosing the appropriate assurance level. It is also important to ensure that a clear communication is given on the part of the CSP to any customer that is then utilizing their cloud service, with respect to proper utilization of the selected services.

Increased assurance can be provided by comprehensive security objectives, defined assessment periods, and an established program as prescribed by the EUCA. Figure 5, conceptually demonstrates this next.

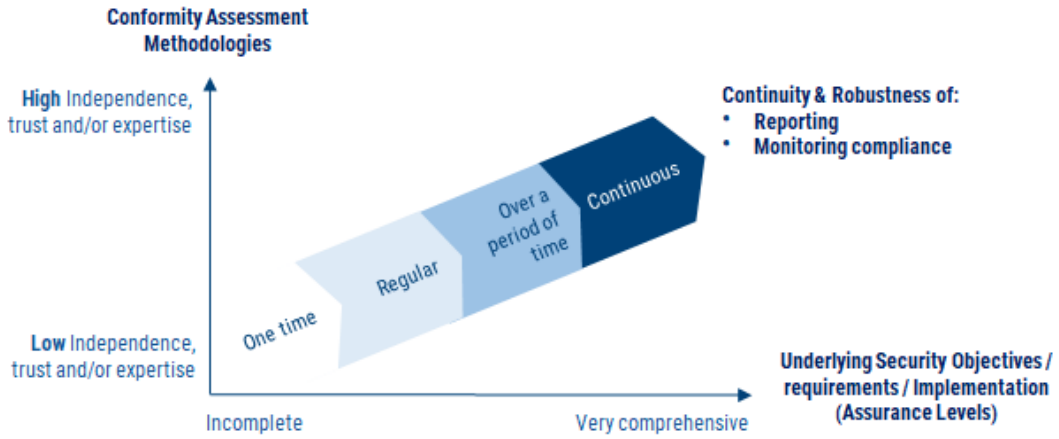

Figure 5. Dimensions of the envisioned CSPCERT scheme

With each risk level, ENISA may consider data localization requirements to be another factor for low, substantial or high. The CSPCERT WG recognizes this variable, as a component concern that can impact innovation and the free flow of data, which in turn can impact on the cloud adoption rates. The EUCA was established to provide, among other aspects, a common framework for the EU, encourage cloud adoption rates, spur investment in the digital single market, and encourage security, privacy and transparency across cloud platforms. Given these factors, data localization, privacy and free flow of data are also components that should be addressed by ENISA.

REC14: ENISA, should as part of this scheme, establish clear guidelines on data localization, privacy and free flow of data requirements that are not in conflict with EU regulations. It is recommended that any requirement, which ENISA may recommend, be harmonized across all member states so as to not impact cloud adoption and investment.

Justification: CSPCERT WG recognizes the establishment of the Regulation on the free flow of non-personal data [15]. As such, this recommendation simply highlights that no final scheme should be in conflict with any data regulation and indeed should support its implementation.

REC15: In the presence of legal data localization requirements, the appropriate level of assurance should be selected based on the recommendation of the relevant authority and applicable legislations.

Justification: Requirements in relation to data localisation can be defined explicitly in legislation, or they can be imposed by the competent authorities, such as supervisory bodies or sector specific regulators. In this case, such requirements can potentially be more easily addressed by leveraging the guarantees provided by a specific level of assurance under the proposed scheme.

The risk assessment process maps the level of the risk based on the probability and the impact of a threat in a risk scenario, which needs to be mapped to the risk assurance level based also in the risk appetite or level of maturity of the end user. The table below is only an example of some cloud service area and risk scenarios level priorities mapped to a level of assurance with the intention of explaining the need to provide a guideline for end-users of cloud services on how to choose their level of assurance.

Table 2. Example of a selection of a Certification Level of Assurance based on risk scenarios and risk assessment taken by an end-user for a Cloud Service

Area / Risk assessment level priority	Assurance Level of Certification	Example of Data / Services
Personal / low	Basic	Cloud services used to support non-mission-critical or non-safety-critical services, and/or to process, share and store data generated by consumer IoT services and applications, or any other services leveraging open/public/non-sensitive data (e.g. recreational IoT applications - connected lights, games and toys -, home automation without safety impact, video and media streaming, personal web page hosting…)
Personal / moderate and high	Substantial	Cloud services used to support potentially mission-critical or safety-critical services, and/or to process, share and store data generated by consumer IoT services and applications, or any other services leveraging not-public/sensitive data (e.g. IoT

Area / Risk assessment level priority	Assurance Level of Certification	Example of Data / Services
		applications and home automation with safety issues (heating settings, connected alarms…).
Business / low	Basic	Cloud services used to support business processes which are not substantial or critical for the survival of the enterprise.
Business / moderate	Substantial	Cloud services used to support important processes and/or to process non-mission-critical data. Examples include: ● Telecommunication/telepresence services ● Accounting services ● Payroll services ● Payment services ● Credit card clearing activities ● Security services for Substantial
Business / high	High	Cloud services used to support mission-critical processes and/or to process, share and store sensitive and regulated data. Examples include: ● patents, core systems, ● Intellectual property and data on critical domains that ensure a cutting-edge advantage on the economic scene thus need strong protection against industrial espionage ● management services on critical infrastructure ● Security services for High
Societal/ low and moderate	Substantial	Cloud services used to support business processes/applications and/or to process, share and store data related to sales and e-commerce. General business services to support communication or secure systems.
Societal/ high	High	Cloud services used to support business processes/applications and/or to process, share and store data related to: ● Critical Infrastructure (Core financial services being deployed in the CSP) or industrial process and Digital Factory (Industry 4.0, or event 5.0); ● Further eIDAS identity services at a High level, that could use cloud computing;

Area / Risk assessment level priority	Assurance Level of Certification	Example of Data / Services
		• Medical records, which by design needs a high level of security.

In the end, the risk assessment is performed and endorsed by the cloud service customer, which is the final risk owner responsible (Due care) for deciding the assurance level that is required for their own needs. Sometimes, an assurance level may be forced through regulation, for example to critical infrastructure sectors. However, defining precisely which assurance level is suitable to which sector is beyond the scope of this document.

REC16: Considering the variety of application and risk appetite, the definition of three levels of assurance: basic, substantial and high, is required in the CSP service certification scheme.

Justification: CSPCERT WG is recommending that the EUCA classification on assurance levels remain classified as basic, substantial, and high. The analysis of the body did not elicit any outliers that would need to be addressed in an added assurance level.

REC17: ENISA and the European Commission should engage regulatory and supervisory bodies with a mandate under Union or Member State law in the Stakeholder Cybersecurity Certification Group defined in Article 22 of the EUCA to explore opportunities where they can rely on certification frameworks to address regulatory compliance requirements where appropriate. The bodies should represent various relevant industries, including e.g. the financial industry, health care, data protection and government.

Justification: As part of their tasks indicated in Article 22, the Stakeholder Cybersecurity Certification Group shall *"assist the Commission in the preparation of the Union rolling work programme referred to in Article 47*" and "*issue an opinion on the Union rolling work programme pursuant to Article 47(4)*". The involvement of regulators and supervisors -- as far as they are not already represented in the ECCG (Article 62) -- ensures that compliance requirements are considered in the consultations.

A risk assessment process is always managed by the risk owner. At times, a specific regulation can establish risk assessment mandates. Regarding the domain considered, some extra requirements might be identified by the risk owner or a regulatory entity in this domain. In this case, the additional requirements should be added to the statement of applicability of the certificate. For example, industry specific controls (healthcare, critical infrastructure) or governmental regulated markets (defence, intelligence,) can be vetted during the certification process.

REC18: The certification of a CSP Service, according to an assurance level, should provide a common secure baseline on top of which various risk owner(s) or critical sector regulation(s) can add additional requirements, depending on their risk appetite.

Justification: CSPCERT WG recognized that overlays or added Security Objectives, would at times be warranted based on the risk owner, sector, or risk appetite of the cloud service customers or

regulators. In these cases, the recommendation here is to simply allow for those added Security Objectives in addition to the existing certification. This can be done as part of the certification of the service so that it carries both the assurance level recognition in the certification and the overlay; or, an add-on could be simply done as part of single use cases on the part of the market and customer engagement for the cloud service. Figure 6 provides an example of how this could be achieved.

Figure 6. CSP certification perimeter and addition of new sectoral requirements

Paragraph 8 of the Article 52 allows for the definition of evaluation levels that would correspond to any of the three assurance levels. The final certification scheme should support that core baseline upon which other sectors can then build upon.

REC19: It is advised to focus the initial ENISA's effort in setting up a generically applicable scheme, based on three levels of assurance. CSPCERT WG would recommend that ENISA foresees extensions of the baseline scheme so to allow for sectorial or cross-sectorial specific requirements.

Justification: CSPCERT WG recognized that there could be misdirection applied to assurance levels within the early creation and adoption phase. The recommendation is to adhere to the EUCA, and to not create sub-levels of assurance and evaluation within basic, substantial, and high. If at some point in time, as the certification matures this need is detected, then it could be added in the normal governance and review of the certification. The recommendations are that in the initial creation of the certification, it should be avoided to decrease confusion for the certification adoption and utilization efforts.

3.3.2 Characteristics and requirement for the assurance levels

The three assurance levels foreseen by the EUCA should cover the security objectives described in the Article 51, which are transcribed to the cloud computing. Article 52 gives assumptions regarding the threat level, the level of the countermeasure required to fulfil these objectives and the depth of the evaluation tasks for each assurance level (basic, substantial and high). The exact text coming from the EUCA is presented in italics.

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

[3] PCI DSS Logo is governed by the PCI Security Standards Council, see: https://www.pcisecuritystandards.org/.

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.

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 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.

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 cyber-attacks 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 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.

These requirements are summarized in the following table below:

Table 3. Cybersecurity act's assurance requirements and their correspondence to the different levels

EUCA Assurance Requirement interpretation	**Basic**	**Substantial**	**High**
Meets the corresponding Security requirements to the assurance level [...]	Yes	Yes	Yes
Designed to mitigate [...]	known basic risks […]	known cyber risks […]	The risk of state-of-the-art cyber attacks
Designed to deter attacker that have [...]	Not applicable	Limited Skills and resources.	Significant skills and resources
Includes technical documentation for review [...]	Yes	Yes (implicit)	Yes (implicit)

EUCA Assurance Requirement interpretation	Basic	Substantial	High
Reviews the non-applicability of publicly known vulnerabilities [...]	Not applicable	Yes	Yes
Has implemented the necessary security objectives for the assurance level [...]	Not required	Yes	Yes, at the state-of-the-art
Assessed offer resistance to skilled attackers via penetration testing [...]	Not required	Not required	Yes

The EUCA requires that the "*respective required security requirements are met for each assurance level*". The CSP Service certification, like other existing certification schemes for cloud computing, is based on the strict conformance to a predefined list of controls.

REC20: It is advised to keep a consistent set of controls objectives (derived from the security objectives from Milestone 1 - see Annex 1) across the three levels of assurance. Instead, the technical controls/specifications implemented to satisfy the requirements of the control objective should vary and be more stringent depending on the selected level of assurance (High, Substantial, Basic).

Justification: Consistent control objectives, as laid out in Milestone 1, are a key component to the success factor for a certification effort. In the final recommendation from ENISA, there should be continuity between the consistency of the initial recommendation, as well as the ongoing maintenance of the certification scheme.

REC21: Penetration testing is the responsibility of the CSP. During the conformity assessment, the design and the results of the pentesting should be reviewed for Substantial and High by the auditor.

Justification: Article 51 of the EUCA requires a component for penetration testing. It is recommended that penetration testing, at a minimum, be a required component for Substantial and High certifications in the final scheme.

For each assurance level, specific evaluation methodologies including penetration testing, and the governance models should be dealt here, in order to assess that the security level required is reached.

Finally, the certification scheme being recommended in this document should allow for differences in the individual assurance levels by:

- Tailoring the methodology used for the evaluation and its depth to the pertained threat level for a given assurance level (covered in Section 4.4 of this document)
- Adding specific requirements for penetration testing, where required (covered in Section 4.5 of this document),
- Managing the cloud certification schemes through a governance model which is specific to an assurance level and commensurate with its stakes (covered in section 5 of this document on SGOV).

3.4 Ensuring EU - wide recognition of certificates through consistency of assurance levels

The conclusions of an assessment/audit report rely on the professional judgement of the evaluator to assess whether a requirement in the security framework is met or not. In order to keep their judgement as objective as possible and to avoid ambiguous or conflicting conclusions, assessment guidelines (e.g. evaluation criteria) should be included in the certification schema. Moreover, it should be assumed that any human-led audit could include a subjective conclusion, due to the fact that they rely on their professional judgement when it comes to interpret if a certain technical or organisational security control satisfy a certain requirement within a specific technological environment and given a required level of assurance. Some of the factors that can influence an auditor's conclusions are:

- Skills of the auditor rating a criterion;
- Cognitive bias and mood affecting the judgement of the auditor;
- State of mind of the evaluation body / certification body;
- National implementation of the considered methodology;
- Other factors…

While implementing a certification scheme, consistency between all the judgements made by all the evaluators that pertains the evaluation needs to be ensured. The gaps in consistency between different conclusions for similar evaluated object is called fidelity. The following types of fidelity can be distinguished:

- *Internal fidelity* of the judgement, which means that the same evaluator, evaluation body or NCCA will come to the same conclusion under different external circumstances;
- *External fidelity* of the judgement, which means that two different evaluators, evaluation bodies or NCCA, or a combination thereof, will come to the same conclusions under similar external consistencies.

The higher the fidelity is, the lower the risk of encountering subjective and interpretations discrepancy in the judgment of the evaluator.

REC22: ENISA, as part of their final scheme, should define an acceptable level of trust in the conclusions of an evaluation report, for each assurance level.

Justification: To ensure a proper recognition of a certificate, the fidelity of the judgement of all the evaluators need to be enhanced, in order to minimize the acceptable error level for a given assurance level. All the bias induced by these subjective factors should be contained within acceptable limits, regarding the assurance level targeted, by different measures. CSPCERT WG therefore recommends that ENISA should:

1) Define detailed guidelines for auditors, and

2) Reinforce the monitoring role of the Scheme Owners/Accreditation Authorities that would need to verify in their annual random audit if a certain Certification Body / Auditor is following the auditing guidelines (for example, ISO/IEC 17065).

Many leverages can be used in order to minimize the judgement errors underpinning an evaluation report for a given assurance level. These include to:

- Ensure the security framework has the appropriate level of detail with respect to the assurance level, which also would drive enough supporting documentation guidance for that assurance level audit. A level of bias can be avoided in an audit evaluation with some measure of instructional audit data as it relates to the Milestone 1 security objectives.
- Reinforce the governance model to ensure internal and external fidelity between the scoring, lower the standard deviation for the scoring and raise for all the criteria, the expectable level toward the reported level in the certificate.
- Ensure a peer reviewing mechanism that helps to harmonize the practice and skills between similar stakeholders (e.g. evaluators and auditor, NCCA), thus ensure better fidelity of the quotation of the internal criterion and reduce the standard deviation.
- Review thoroughly by a supervising authority the certificate issued, in order to harmonize the quotation on criteria and to increase its external fidelity.

Note that raising the technical level of objectives and controls requires that the skills of evaluators are aligned with the state-of-the-art. Consequently:

REC23: It is advised for assurance level substantial and high, which rely on more demanding security objectives, to have an enhanced governance level that ensures that the skillset for the evaluators are less subject to interpretations and judgement errors during the evaluation.

Justification: However, state-of-the-art is subject to personal interpretation, thus it might induce to a high-level error, as there is a direct correlation between these two variables.

Existing conformity assessment bodies (CABs) such as certification bodies, inspection bodies or testing laboratories should continue to be able to be used for the substantial and high levels of certification by establishing an EU licensing authority under the rules of the ENISA governance recommendation. For High, the existing model of national accreditation authorities would likely suffice as the certification mechanism.

Under the EUCA there are currently no existing CABs, so all CABs will need to be accredited. This applies not only to certification bodies, but also to inspection bodies or testing laboratories as well as auditing firms.

REC24: For applications that are deemed highly critical, the highest possible confidence level is required, and discrepancies between the assessment pertaining to the delivery of certificates less tolerated. For less critical applications, this fidelity level could be lowered without harming the credibility of the certification scheme.

It is advised to keep a good balance within each assurance level between the technical stringency of the implementation of the controls, cost of the assessment and measurements used to raise the fidelity of the assessment.

For the high assurance level, ENISA should implement and leverage any measures that would help to raise the fidelity between conformity assessments, thus the overall confidence level in the certification (e.g. governance, guide, and so on).

For the lower assurance level, the confidence level expected is lower. Consequently, ENISA should rely on simple technical requirements for the control implementation, in order to contain the cost of

measures needed to regulate the fidelity of the assessment (e.g. governance, guidance, as depicted above).

Justification: Discrepancies in assessment are more likely to occur on complex and highly technical requirements regarding the implementation of the security objectives. Moreover, reaching a high security level often relies on the usage of complex mechanisms that are compliant with the state-of-the-art and could be difficult to assess.

Finally, confidence in a certificate is related to how the security experienced is when using the cloud service in respect to the security claimed by the certificate. The higher the fidelity is, the lower this gap is.

To this end, the security level of a certificate, the technical level required for the implementation of its controls and the fidelity of the assessment are correlated.

For the high level, the EUCA left no room for the compromise regarding security, as the requiring implementation of the control and the architecture of the service certified are to be compliant with the state-of-the-art. For other levels, a compromise can be made between these variables in order to keep a good balance between these variables and the cost of a certification / certification model.

REC25: For the high level, it is recommended that the NCCA endorses the final audit reports and the issuance of the certificate, in order to be able to harmonize the consistency of the evaluators' judgement, regarding the conformity against different controls.

Justification: The NCCA is in a position to endorse all evaluation reports issued by various CABs under its control. NCCAs are also impartial. Consequently, they can control and ensure a certain level of consistency between them, while instructing the issuance of its certificates.

The governance models described in section 5.4 (High), 5.5 (Substantial) and 5.6 (Basic) take into account these recommendations in their proposal.

Peer review is required by Article 59 of the EUCA and is part of the governance model for the NCCA. The recommendation related to this review between peer is addressed in the SGOV part of this document. (see Section 5).

Recommendations regarding the review of the evaluation report and the harmonization of the issued certificate are dealt in Section 4.2 of this document.

REC26: The assignment of controls and methodologies should be done in a way that each assurance level is nested within each other, so that the following occurs:

- A certificate at the high level should comply with the controls and methodologies used for the substantial and the basic level;
- A certificate at the substantial level should comply with the controls and methodologies used for the basic level;
- The final certification mechanism should allow for a natural progression, through enhanced control implementation and control validation (which is part of any normal auditing and testing effort) for the service to progress to the next assurance level without restarting under a fully new testing or auditing process.

Justification: Clear guidance for CSPs to have a clear path to move from one level to another level of assurance can encourage consistency and clearness across the EU for a transition from basic, to substantial, to high assurance levels.

4 CSAR Coverage Cybersecurity Act requirements regarding the CSP certification

4.1 Generic requirement of the scheme

This section covers articles 54 and 55 of the EUCA.

Article 54 lists themes and topics that should be addressed while defining a new certification scheme.

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;

(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;

REC27: The purpose of the scheme is to provide the user of cloud services with a statement about its scope, reliability and security in accordance with regulations. The purpose of a Conformity Assessment Certification is to enhance the credibility (or confidence or trust) towards stakeholders of a statement expressed by a cloud service provider (CSP) that its cloud service (including those from sub-service providers) meets the requirements of a predefined set of control objectives and a related set of measures, equivalent to the requirements proposed in Milestone 1 (Details in Annex 1).

Justification: ENISA should establish a clear definition of the scope of the certification scheme, the conformity method for each assurance level, the stringency of the security controls, guidance and reference documents, etc., and make them publicly available.

(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 of 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

REC28: Consider the security categories and additional specifications for high- and low-level security objectives provided in the Milestone 1 document (see Annex 1) based on the analysis of existing standards.

Justification: CSPCERT WG has already performed an initial mapping and gap analysis of existing public certification schemes coming from EU member states as well as international standards such as ISO / IEC 2700x that should be extended to include additional schemes and standards.

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

REC29: For CSPs, three levels of assurance based on the outcome of the risk assessment performed, are permitted. These levels are Basic, Substantial and High.

Justification: CSPCERT WG recommends adhering to the EUCA and define three levels of assurance.

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

REC30: Purely self-assessment leading to a Statement of Conformity should not be permitted due to the risks arising from the use of cloud computing services. However, the basic assurance level should be founded on an evidence-based conformity assessment as described in Annex 2.

Justification: Due to their complexity, business importance and the interconnection/reliance of Cloud services, the adherence to the cloud security certification scheme should be verified by a neutral (or independent) institution. As noted by the EUCA in Recital 79, self-assessment should be considered to be appropriate for low complexity ICT Products, ICT Services or ICT Processes that present a low risk. The CSPCERT WG considers that the usage of cloud services can arise high risks to the public.

(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;

REC31: Specific requirements for Conformity assessment bodies are covered in section 5 and should be adopted as part of the final certification scheme.

Justification: Under the EUCA there are currently no existing CABs, so all CABs will need to be accredited. The conditions presented in Section 3.4 apply not only to certification bodies, but also to inspection bodies or testing laboratories as well as auditing firms.

(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;

REC32: Annex 1 presents a set of security objectives that should be taken into consideration by ENISA in the final EU-wide certification scheme.

Justification: CSPCERT WG has defined a consistent set of security objectives, along with a supporting methodology, to include further security objectives as needed.

(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;

REC33: The CSP should provide full insight documentation of any service(s) and the way they have organized themselves to be able to adhere to the Milestone 1 objectives as well as which control measures have been implemented. A template has been provided in the 'Annex 4: Template Report CSP Management Assessment' to support this recommendation.

Justification: The EUCA recognizes the clear need for transparency on the part of the CSP when that CSP is seeking any certification of a cloud service. The recommendation supports requirement (h).

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

REC34: Upon discussion, the recommendation of the drafting team is that no mark or label is applied in the context of this scheme. The principal reason behind this recommendation is the need for a careful risk assessment to be conducted on a case by case basis to determine the need for a High, Substantial or Basic level of assurance under this scheme. The need for this risk assessment implies

that labels or marks are likely to be misunderstood or misinterpreted as providing a guarantee of appropriate assurance.

Justification: CSPCERT WG recognizes that labels or marks can be misunderstood or misinterpreted in the context of the cloud security certification scheme.

(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;

REC35: CSPCERT WG advises to follow the recommendations regarding the monitoring of compliance with the requirements of the EU certificates and the mechanisms to demonstrate it provided in Sections 5.4.2.1, 5.5.5 and 5.6.4 of this document.

Moreover, it is advised that each assurance level foresees the implementation of monitoring mechanisms and processes of the issued certificates.

Justification: Monitoring of any certification is mentioned under the EUCA, which is a commonly accepted practice for any secured cloud offering. CSPCERT WG recommends that the level of monitoring is commensurate with the level of certification, i.e. Basic, Substantial, or High.

(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;

REC36: Sections 4.2 and 4.3 provide a set of recommendations to grant, maintain, and ensure the continuity and the renewal of any given certificate. The recommendations of those sections should be followed, as ENISA issues the final guidance for the certification scheme.

Justification: CSPCERT WG recognizes that conditions for issuing, maintaining, and ensuring the continuity of a certificate issued to a cloud service is a key objective of the EUCA. This recommendation is in support of that EUCA language as noted in (k) above and directs the reviewers to key sections of this document in support thereof.

(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;

REC37: As mentioned in Annex 4 of this document, as part of the certification scheme, it should be ensured that CSPs obtaining a certification under the scheme:

(i) Warrant and represent that they are fully aware of, and understand all requirements of the scheme relating to the relevant service;

(ii) Warrant and represent that, to the best of their knowledge and understanding as a professional CSP acting with appropriate diligence, their service complies wholly and entirely with all requirements of the scheme;

(iii) Warrant and represent that, to the best of their knowledge and understanding as a professional CSP acting with appropriate diligence, any information in relation to compliance with the requirements of the scheme that they have provided to a conformity assessment body, to a National Cybersecurity Certification Authority (NCCA), or to any other third party charged with verifying or assessing compliance with the requirements of the scheme, was accurate and up to date at the time of submission;

(iv) That they should not claim to hold any certification in relation to a certified service towards any third party (including the public) in relation to the scheme as soon as they become aware that the service is no longer compliant with all requirements of the scheme, or if it is reasonably likely that their service is no longer compliant with all requirements of the scheme; and

(v) Will hold any harmed third parties harmless for proven damages resulting from a violation of these requirements as far as required under applicable law and under the terms agreed with the users of the service.

Justification: Annex 4 of this document provides a template to be used by the CSPs to provide information to any review body in the case of Evidence Based Self-Assessment as well as to any conformity assessment body to be able to execute their conformity assessment. Furthermore, it also provides evidence of the self-assessment process executed by the management of the CSP. Rules for ICT products and services are recognized in the EUCA as a key requirement, to which this supports as noted in (l) above.

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

REC38: Consider including as a set of minimum Security Objectives as those already defined in Milestone 1 document (e.g. section 3.7 'Operational security'). In addition to what OS.7 says from the section 3.7 Milestone document, a CSP should adhere to a vulnerability disclosure process.

Justification: The security objectives have already been defined to meet this requirement in the Milestone 1 documentation effort conducted by CSPCERT WG.

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

REC39: That the final certification scheme requires a 7-year period for retention of records.

Justification: CSPCERT WG recommends that no record retention scheme should exceed a 7 year period, and in no case should exceed it as required by superseding European regulation or law.

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

Several schemes exist, international (some translated into European Norms or EN) such as ISO/IEC 27000 family [12] [6] [7], public national such as BSI C5 [4], ANSSI SecNumCloud [3] and ENS [16]. These are complemented with a set of public and private international and national standards and schemes

that define, wholly or partially, a set of security objectives for cloud services. An initial mapping and subsequent gap analysis of several of these schemes is shown in Milestone 1 document, Annex 1a.

REC40: It is recommended for ENISA to show how the Security Objectives of the adopted EU-wide cloud certification scheme relate to the other existing schemes, when relevant. ENISA should therefore extend the gap analysis following the methodology described in Annex 1, which has been designed to accommodate further schemes, generic or sectoral.

Justification: There exist several schemes in the context of cloud security that should be taken into consideration when designing the EU-wide certification scheme, as done by the CSPCERT WG group and presented in Annex 1 of this document.

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

(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;

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

REC41: For High and Substantial offers, with the unique threat landscape of cloud services, it is recommended that continuous auditing is followed by the CSPs or an annual audit of cloud services is performed at minimal.

Justification: Given the ever-evolving threat landscape for cloud services, a continuous certification process (which may include a continuous monitoring component) should be adopted as part of the requirements for a substantial and high certification. It would be up to ENISA to craft where these delineations would fall for the final recommended scheme.

REC42: For Basic offers, an evidence-based conformity assessment certification should not exceed more than a 3-year cycle provided that a control check is performed every 12 months. ENISA should clarify what would trigger a new out of cycle review.

Justification: At a minimum, for rigor of cloud certification on an EU-wide basis, even at a Basic level there must be a limit to the application of a Basic certification. At a 3-year cycle the certification would align to very basic certification requirements and international norms.

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

REC43: A responsible disclosure policy related to the withdrawal of the certificate should be established for the CSP Certification scheme. The right balance should be ingrained within the final scheme, in order to cope with security, intellectual property and the reputation of the CSP. Information related to non-conformities should be included in any audit report, which is shared only between the auditee and the auditor/certification body. The public and stakeholders (e.g. cloud customer, partners, regulators) should have the right to know when a cloud service is NOT longer certified.

Justification: Disclosure of an invalid certification should be the result of the ongoing certification process so as to inform and protect consumers, regulators, CSPs and any other relevant stakeholder.

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

REC44: The topic of mutual acceptance of third-party certification schemes outside the EU is a political issue. ENISA, as part of their final recommendation to the Commission, should recommend a governance model for mutual recognition of non-EU third-country cloud certifications.

Justification: Given EU membership in the WTO, it is not unreasonable to expect that the EU will receive requests for other international certifications to be reviewed with the same rigor and relationship to the common scheme being proposed in the EU. ENISA should plan ahead for other common non-EU frameworks.

(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;

REC45: The mechanisms for peer reviewing for the assurance level high are described in the Section 5.2

Justification: The EUCA calls for peer assessment mechanisms to be part of the final recommended scheme, to which CSPCERT WG has produced some recommended guidelines in Section 5.2

(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.

REC46: The cloud service provider should supply and update the supplementary cybersecurity information that is described in Article 55, for all assurance levels.

This information should be made available on the CSP provider's website and found easily by the end user and other relevant stakeholders.

It is recommended to define a common format for this information, to have them published and linked aside the certificate in a database maintained by ENISA.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

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.

REC47: In accordance with the terms of the EUCA, no part of the scheme should contain a requirement which is knowingly drafted in a manner that would contradict any applicable legal requirements.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

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 the requirements of that legal act.

REC48: In accordance with the terms of the EUCA, certificates or statements of conformity which are issued in compliance with the terms of the scheme, and which are still valid in relation to those terms, may be used by the CSP as an element to support the demonstration of their compliance with the terms of specific legislation, provided that the legislation permits such use of the certificates or statements.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

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.

REC49: In accordance with the terms of the EUCA, certificates or statements of conformity which are issued in compliance with the terms of the scheme and which are still valid in relation to those terms, may be used by the CSP to create a presumption of compliance with the Member State's level legal requirements, provided that the Member State's legislation grants such a legal effect to the certificates or statements.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

Article 55 states:

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;

REC50: The CSP should provide end users with supportive information, e.g. best practice guides, predefined secure configuration sets or choices thereof. The extent may vary depending on the respective offered certified service model.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

(b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;

REC51: The requirement of the EUCA is very much related to products. Unsupported cloud services are the exception, because security breaches may lead to a financial loss for the CSP. Security support usually ends with end of life of the cloud service itself. It is recommended that the CSP informs the customer, via agreed communication channels in a timely manner or by accordingly to the national regulations that define mandatory reporting and the defined process, if the agreed security level is no longer provided or the offered certified service is discontinued.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

REC52: The CSP should provide an interface to receive vulnerability information from customers and other relevant stakeholders, e.g. messages over a portal of the CSP, a specific email account or other communication channels. As vulnerability information is sensitive, the communication channel should be adequately secure at least for highly sensitive data that could be used for a successful attack of the cloud service.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

(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.

REC53: The CSP itself can publish a list of the vulnerabilities of the certified cloud service or to a reference to online Common Vulnerabilities and Exposures (CVE) repositories.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

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.

REC54: The CSP should provide the necessary information, unless the cloud service end of life is earlier than the issued European cybersecurity certificate.

Justification: CSPCERT WG recommends following the guidance supplied in the EUCA.

4.2 Issuance of certificates

An EU-wide cloud service provider security certificate issuer should be using one of the Conformity Assessment Methodologies described in Annex 2.

Typically:

- Certificates issued by a Conformity Assessment Body (CAB), accredited according ISO/IEC 17021 [17], are for an organisation or organisations providing a service, that have chosen to implement a management system for planning, achieving and improving a set of objectives of a particular area of relevance to the organisation (e.g. quality, environment or information security).
- Certificates by a CAB accredited according ISO/IEC 17065 [18] are related to specific products, processes or services, to which the same specified requirements, specific rules and procedures apply. While the provision of a cloud service encompasses more than the manufacture of a simple discrete object, ISO/IEC 17065 [19] equates its applicability of a product to that of a service or process. Related, the General Data Protection Regulation (GDPR) also requires the application of ISO/IEC 17065 for a CAB to perform a conformity assessment.

However, any CSP will need to have implemented a well-designed and operating information security management system (ISMS). The well-established ISMS certification scheme using ISO/IEC 27001 [20] may be considered a requirement of substantial and high level of CSPCERT certification scheme.

A cloud service certification should be built according to the principle of inheritance of the assurance level, i.e. a SaaS hosted on an IaaS would obtain the level of assurance granted by the certification of the IaaS. However, in order for a SaaS or a PaaS to be able to achieve a higher level of assurance provided by an underlying PaaS or IaaS, additional assurance mechanisms need to be implemented and these in conjunction with the overall higher service needs to undergo an additional conformity assessment. In order to enforce the certification inheritance principle, it is essential that the certification value chain is based on an adequate level of transparency and accountability. Here, the contractual flow down and evidence of right to audit/access audit reports would suffice as part of those added reviews under the audit review process.

In order to lessen the burden of an additional certification, evidence gathered during an audit process for a CSP service certification scheme should be able to be reused as evidence for other certifications or vice versa.

Making a cost effective and efficient CSP service certification scheme available that provides a recognisable market value will increase the competitiveness of those services that achieve the certification.

REC55: ENISA should develop a mechanism that enables a CSP to move from Substantial to High, without a complete change of assessment methodologies.

Justification: The final CSP service certification scheme should be designed in such a way that CSPs can move to a higher level of assurance without an extremely high investment, by accepting, when appropriate, the reuse of evidence.

4.3 Maintenance of certificates

The CSP service certification scheme that is being established through the EUCA will become a European Union program that will standardize the way in which cloud computing services are certified within the European Union. The recommended maintenance of those certificates is discussed in this section.

REC56: ENISA should develop a mechanism that would account for any complaint handling processes that would be a by-product of the certification issuance and/or certification maintenance program, in support of Recital 102 of the EUCA.

Justification: Clear procedures and guidance must be published for all stakeholders to have a common understanding on how the certifications will be maintained and renewed, as well as on the management of complaints and appeals.

Certifications should be issued by one of the following:

- The National Cybersecurity Certification Authority;
- A delegated authority such as a Certification Body.

Certifications are given to the relevant CSPs in line with the defined Conformity Assessment methodology. Certifications, once issued, should be required to be maintained, at least, in line with such methodology and taking into consideration the aspects listed below:

- CSPs compliance to the certification scheme should be reviewed and/or reassessed in line with the Conformity Assessment methodology.
- The certificates issued should only be applicable to the services agreed by the CSPs and the National Cybersecurity Certification Authority during the conformity assessment process.
- CSPs should be able to update the scope of the certification applicability during the continuous auditing process, i.e. CSPs can add and/or remove services from the scope of the certification assessment.
- CSPs should have the ability to review the assurance levels applicable to them in consultation with the National Cybersecurity Certification Authority. This should be based on changes to products or services offered by the CSPs.
- CSPs should have a right to appeal to the National Cybersecurity Certification Authority, or an authority established by ENISA, for any:
    - Discrepancies generated out of the continuous auditing process;
    - Complaints arising from the outcome of the certification assessment.
- The National Cybersecurity Certification Authority should have a well-defined complaint and enquiry handling mechanism to enable resolutions of concerns and queries from the CSPs.
- Complaints and enquiries should be resolved within a fixed timeframe by the National Cybersecurity Certification Authority, and where required, the National Cybersecurity Certification Authority should engage with the relevant CSP.

4.4 Assignment of controls and methodologies for each assurance level

The assignment of controls and methodologies, as noted in Recommendation 26 (namely, the last recommendation in Section 3) should be followed.

This implies that similar security objectives (see Milestone 1 - Annex 1) related to the cloud service certification are shared across assurance levels. Moreover, the requirements related to the security objectives described in the Milestone 1 document should be declined in different stringency levels according to the assurance levels. The depth of the evaluation methodologies used and described in the Milestone 2 should also vary according to the assurance level.

The figure below shows how the different controls, corresponding requirements (derived from Milestone 1) and methodologies are declined across certification levels.

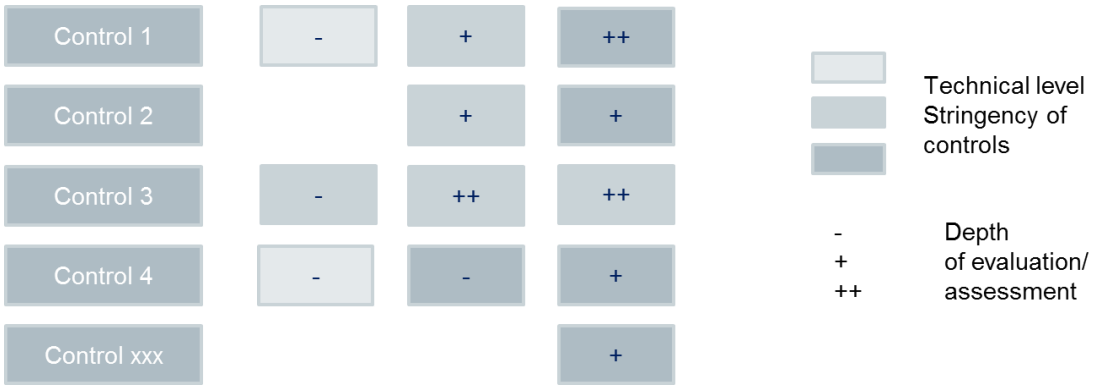

Figure 7. Example of Combination of controls, corresponding Requirements and methodologies.

Further recommendations and explanations regarding the controls and the methodologies are given in Annex 1 and Annex 2 of this document.

4.5 Pentesting

While the EUCA considers penetration testing mandatory at assurance level High, if properly done, this practice can benefit other assurance levels. However, it is to be noted that a penetration test relies heavily on the skills of the auditor. Besides taking into account the state-of-the-art attacks, the scope of a pentesting should be properly determined so as to be effective and useful.

Pentesting shall not be mistaken with the concept of only challenging an infrastructure or a service against state-of-the-art attacks performed by the auditor. Pentesting is a service delivery that should be formalized and should include specific steps and meet specific requirements, for example:

- Defining the precise perimeter and scope of the audit;
- Defining proper test plans;
- Agreement with the audited party of the tests to perform;
- Formal and proper feedback on the penetration testing;
- Proposal of countermeasures, fixes and improvements regarding the results of the penetration testing;
- etc.

REC57: It is advised to rely on existing internationally recognized frameworks to properly manage the penetration testing activity for cloud service evaluation. Penetration mechanisms, like PASSI (France), CREST (UK), FedRAMP (USA), TIBER (NL), TIBER-EU(ECB) or NIST 800-115, should be considered and used in the framework of CSP service certification. It is not necessary for rely on pentesting auditors qualified under national frameworks, but they should, however, be qualified under a final ENISA recommendation.

Justification: Defining a proper pentesting framework could be a certification scheme by itself. Consequently, it is advised to leverage on existing national frameworks at this time to properly determine the scope of this activity, as well as to ensure their consistency between CABs and NCCAs and through time.

At the high assurance level, one's NCCA penetration testing shall be recognized as equivalent and as efficient as the others in order to ensure proper mutual recognition of the certificate.

REC58: For the high assurance level, penetration testing practice and framework should be shared and agreed between NCCA.

Justification: Sharing a common framework, methodology and state-of-the-art between stakeholders is mandatory in order to achieve a mutual recognition of the conclusions of such evaluation.

Proper governance, as described in Section 5.3 as well as community management and information sharing, as described in Section 5.3.2 would help.

5 SGOV Management of the CSP Service Certification Scheme

Several key steps would need to be taken during the ENISA review period to establish a transition from a state-focused to single market certifications. The Cybersecurity Act and EU Commission intent is to promote an EU-wide certification scheme to enable an EU Digital Single Market. The CSPCERT WG has provided, as a basis of this effort, an EU-based approach to cloud certification.

From the efforts presented in each Milestone, the CSPCERT WG has provided guidance on a future EU-wide certification scheme. As part of Phase 2, ENISA should review the recommendations made in this document, as well as the underlying frameworks, research, and conclusions of the CSPCERT WG.

Three key recommendations to support a transition to an EU-wide certification approach, regardless of CCAL, include:

REC59: The certification scheme should be established and be a mutually recognized certification for all member states as directed in Article 49(1) of the EUCA. Current member state cloud certificates will continue till their expiry date, after which entities will need to certify under the final ENISA proposed scheme.

Justification: While mutual recognition is a political issue, ENISA should recommend the European Commission a mutual recognition governance model to ensure that current existing member states' certification schemes are recognized in other member states until the transition period expires, and the EU-wide certification scheme enters into place.

REC60: ENISA should analyse how the cloud security certification schemes defined in the different member states (e.g. SecNumCloud in France, BSI C5 in Germany, ENS in Spain, and so on) conform to the different levels identified in the EUCA and can become an EU standard, provided that mutual recognition is achieved.

Justification: The transition from existing certification schemes to the EU-wide certification scheme shall be made as easy as possible. Taking into consideration the security objectives defined in Milestone 1 and the conformity assessment methods, ENISA should determine under which level each existing certification scheme is placed, so that CSPs are aware of the level of security in which they are certified.

REC61: ENISA, as part of their final recommendation, should recommend any appropriate transition and/or governance oversight for currently existing cloud certification schemes defined in the different member states of the EU (For example, BSI C5, SecNumCloud and ENS) to encourage certification and cloud cooperation, adoption, and collaboration across member states. Moreover, ENISA should also take into account existing private certifications (EuroCloud Star Audit [21], LEET Security rating [22], CSA STAR [23], Zeker Online [24], etc), as well as ad-hoc experts' opinions so as to add value from the industry current market state-of-the-art .

Justification: For each of the assurance levels (basic, substantial and high) an analysis regarding the transition has been performed. This analysis can be found in Sections 5.4.4, 5.5.3 and 5.6.3 of this document.

REC62: ENISA, should as part of the final schema, consider also add-ons to existing public certification schemes coming from member states that would include additional aspects (e.g. conformity method, levels of stringency in the controls) that ENISA would deem appropriate for those schemes placed in the substantial level in order to be recognized as high. This may be a mechanism for CSPs to move more rapidly from substantial readiness to high, if no path is currently available to easily transition from existing public certification schemes currently classified as substantial, to high.

Justification: The transition from lower levels to higher levels shall be facilitated so that CSPs can move faster to higher levels in order to ensure the highest security levels to cloud consumers. For current certificate holders of currently existing public certification schemes, this shall be eased with the definition of add-ons (e.g. conformity method, levels of stringency in the controls).

5.1 Complaints management

A complaint can concern a broad range of issues, spanning from discussing the issuance of a certificate to aspects related to the management of the certification scheme at EU level. To ensure the transparency of the scheme, it is critical that complaints are carefully and fairly investigated through a robust process.

Any complaint related to the infringement of existing national, European or international laws and regulations are out of scope of this complaint management process and have to be solved by the relevant legal entities.

ENISA should seek to have a transparent complaints procedure in place which would be offered as part of the final scheme. CSPCERT WG also recommends that such a complaints management process includes steps to mediate between the parties, and that such mediation process has a transparent outcome.

For the basic level, the complaint(s) can be first put forward to the monitoring body which will investigate and try to resolve the issue. When no agreement can be found, a complaint request shall be formally recorded by the most appropriate authority to be further investigated.

REC63: A complaint shall be initially formally made to the NCCA of the member state of the issuer. In the case in which the complaint involves this NCCA, the complaint has to be registered at EU level by ENISA.

Justification: The closest independent authority shall be involved first, in order to facilitate the resolution of the issue in a pragmatic way.

Depending on the complaint, it could be qualified and resolved at different level.

REC64: The complaint should be resolved by the NCCA of the issuer in the cases in which it is related to the issuance of a certificate, the approval of a CAB or if it involves processes, certificates or entities that are under the direct supervision of the NCCA.

REC65: The complaint should be first solved bilaterally between the NCCA of the incriminated third party and the NCCA of the issuer, if the complaint is related to a certificate, the approval of a CAB or if it involves processes, certificates or entities that are under the direct supervision of the NCCA of the incriminated third party.

REC66: The complaint should be handled at EU level by the Conciliation Commission, should the complaint involve directly the scheme or two different NCCAs.

Justification: The independence of the authority arbitrating the issue should be ensured, without having to request an arbitrage at a highest level. When an arbitrage is required, no stakeholders involved in the complaint should be part of the decision.

During the arbitrage, each involved party shall have the same level of information related to the case. However, in any case, the content shall remain confidential.

REC67: All evidence related to the issue and used for the arbitrage should be shared between the parties. All stakeholders should commit to ensure proper confidentiality of this shared information through a formal agreement or statement.

Justification: A balance should be achieved between ensuring the confidentiality of the evidence and the need for transparency in the arbitrage process.

In the case of appeal of the arbitrage decision of a NCCA, the case can be brought to a higher level.

REC68: Appeal to a decision can be made at EU level and handled by the Conciliation Commission, like any other complaint.

REC69: In any case, the decision of the Conciliation Commission should be considered as final, and cannot, thus, be reconsidered.

Justification for REC68 and REC69: The Conciliation Commission is the highest authority who can investigate and arbitrate a conflict. Thus, there is no escalation or appeal process that can go beyond.

The independence of the Conciliation Commission shall be ensured.

REC70: The members of the Conciliation Commission should be elected by the Management Committee for a limited period of three years and renewed by a third each year.

REC71: The Conciliation Commission should be composed of six members elected from the representatives of the NCCA of the Management Committee. Theses members should appoint a president, who would be in charge of chairing the Commission but would not be able to participate in the voting.

REC72: Two alternate members should be elected in order to be able to replace one of the Commission members in case of unavailability of one of the regular members, or in the event in which one member is directly implied in the case arbitrated which should be replaced temporarily for the sake of impartiality.

Justification: As the Conciliation Commission is the highest authority for arbitrage, it is mandatory to have stringent rules to ensure its complete independence and the absence of conflict of interest.

REC73: The position of secretary of the Conciliation Commission should be held by an agent of ENISA.

Justification: This recommendation is aimed at ensuring continuity in the recording of a decision made by ENISA.

5.2 Peer review

Article 59 of the EUCA deals with the requirement of peer review.

1. *With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, national cybersecurity certification authorities should be subject to peer review.*

2. Peer review should be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.

3. Peer review should assess:

(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other;

(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);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services or ICT processes pursuant to point (b) of Article 58(7);

(d) the procedures for monitoring, authorising and supervising the activities of conformity assessment bodies;

(e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level 'high' pursuant to Article 56(6) have the appropriate expertise.

REC74: The Peer review should conform to the following objectives and criteria, that have to be settled and agreed first by the Management Committee:

- National governance of the scheme by the NCCA;
- Vetting the conformance of the NCCA against the criteria used for approval of CAB;
- Technical skills management of all national stakeholders;
- Accreditation by a NAB of the NCCA;
- Security management related to the issuance of the certificate.

Justification: The peer review has as an objective to check the skills and the organisation so as to properly manage the scheme. This is so, because since the NCCA issues the certificate at the assurance level high, the peer review should verify that the NCCA fulfils similar requirements than the ones that are applicable to a CAB.

4. Peer review should be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and should be carried out at least once every five years. ENISA may participate in the peer review.

REC75: The peer review process should allow intermediate reviews, for specific cases (e.g. If major gaps have been identified during an audit of a NCCA and should be fixed).

Justification: The peer review can be an incentive for NCCA to help each other to maintain state-of-the-art skills and competencies in the framework of cloud services certification.

5. The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. In adopting those implementing acts, the Commission should take due account of the views of the ECCG. Those implementing acts should be adopted in accordance with the examination procedure referred to in Article 66(2).

REC76: Criteria, objectives and methodology that pertains the peer review on a High level shall be made public and should be defined in an implementing act. They should cover the means and processes that ensure the independence of the peer reviewing process. These should be published by the ENISA on its website.

Justification: Transparency is required to ensure trust in the scheme. However, describing all the fine-grained requirements for the implementation of these criteria as well as the methodology details used for their verification is beyond the implementing act.

REC77: Besides the high-level requirements published as an implementing act, the Management Committee should write, agree on and maintain technical supporting documentation that clarifies and refines the requirements established for the NCCA that are subject for peer reviewing. These details should include both implementation requirements and the methodology used for verifying them.

Justification: As state-of-the-art evolves quickly, the process of maintaining a corpus of detailed requirements should be continuous and should allow to perform quick changes that are shared among stakeholders of the scheme.

REC78: All supporting documents upon which the Management Committee have agreed, should be made public (e.g. on the website of the scheme)

Justification: For the sake of transparency, all the evaluation criteria and the supporting documentation that are not directly specific to a particular entity (NCCA, Member State....) should be made public.

6. The outcomes of peer reviews should be examined by the ECCG, which should draw up summaries that may be made publicly available and which should, where necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.

REC79: The full report related to the peer review should remain confidential, especially what concerns the identified gaps with the defined requirements or objectives. However, the activities and the general outcomes of the process of peer reviewing should be made public for the sake of transparency.

Justification: Although transparency is wished, some confidentiality is required regarding the outcome of the peer review process. The underlying idea is to promote cooperation between NCCAs to achieve a satisfactory level of governance, skills and management of the scheme and not to introduce competition.

5.3 Common Roles and Governance Across Assurance Levels

5.3.1 Comitology and formal groups at EU level

The figure below presents the Roles and Governance model for all levels suggested to ENISA.

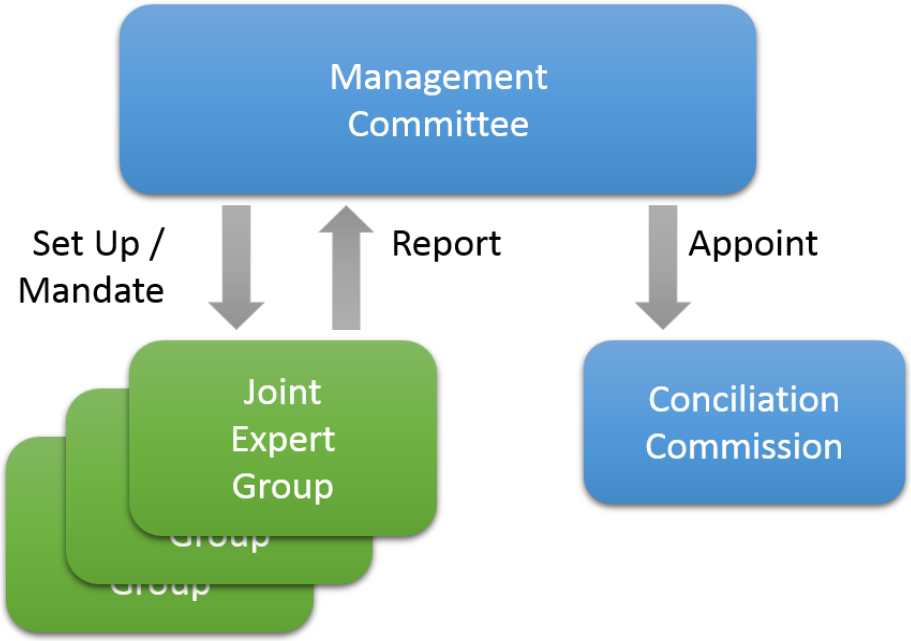

Figure 8. Governance models for all assurance levels

Three major entities are involved at this level:

- The *Management Committee* is a board composed of representatives of the NCCAs and ENISA.
- One or many *Joint Expert Group(s),* that are set up by the Management Committee and assigned to work on specific topics. The Joint Expert Group(s) should bring together various experts from the public and/or private sector as well as representatives of EU or national institutions, depending on their assignment.
- A *Conciliation Commission*, which is appointed by the Management Commission for a limited period of time and plays a key role in case of disputes. The Management Committee should:
  1. Maintain the reference documentation of the controls and methodologies;
  2. Ensure a formal equivalence between the different methodologies that could be used and promoted by the NCCA for the evaluation by:
     i. Approving standards and norms pertaining to the certification of cloud services (as suggested in annex 2);
     ii. Identifying gaps between these methodologies and the requirements for the cloud services certification;
     iii. Agreeing and publishing specific requirements filling the gaps for these standards, in order to ensure mutual recognition of the certificates;
  3. Define the roadmap and agree on the evolution of security objectives/controls and conformity assessment methodologies;
  4. Monitor all assurance levels of the scheme;
  5. Appoint, for a fixed time, from the members of the Management Committee, the members of the Conciliation Commission;

6. Set up the Joint Expert Group(s), as they could be needed;
7. Solve the disputes related to the CSP service certification scheme, as described in section 5.1 (Complaints management).

Each Joint Expert Group appointed by the Management Committee should:

1. Propose the Management Committee updates to the security objectives/controls and conformity assessment methodologies;
2. Identify, share and agree on appropriate and good practices related to cloud services security and pentesting;
3. Analyse and report on specific technical issues related to cloud (cyber)security and/or certification, that are identified by the Management Committee and which could have an impact on the EU-wide CSP service certification scheme;
4. Provide expertise and technical advice to the Management Committee upon request (e.g. to help the Management Committee to establish a roadmap, to analyse the impact on sectorial regulations…)

Moreover, this group could become the appropriate forum to exchange good practices and methodologies among stakeholders of CSP services certification.

5.3.2 Community management

At the high level, the EUCA emphasises the fact that certified cloud services shall conform to state-of-the-art architecture and shall resist to state-of-the-art attackers. For other assurance levels, good and appropriate practices should be shared between all stakeholders.

It means that all stakeholders (CSP, end-users and consumers, CABs) shall share a common understanding and vision on what the appropriate good practices are, regarding cloud cybersecurity in accordance to the considered assurance level.

The creation of a governance model at EU level would help to share views on state-of-the-art methods, practices and architectures between NCCAs. This could be done within specific Joint Expert Groups.

REC80: The Management Board should set up one or more specific expert groups in charge of evaluating and sharing the appropriate good practices, especially the ones on architecture and pentesting or when the “state-of-the-art” is invoked. These expert groups should include all NCCAs and major players in these domains.

Justification: Good practices and state-of-the-art in-service architecture and in pen testing is evolving faster that the pace of writing and sharing academic or normative papers. Consequently, these practices shall be shared orally within a specific community of stakeholders. Moreover, this expert group should include not only all the NCCA, but also any relevant and independent experts for the considered domain (architecture, pentesting, ...) coming from key EU external organisations from public or private sector.

Moreover, the NCCA is in charge of managing the scheme at national level. Thus, it has a key role to play nationally to share this state-of-the-art with all its national stakeholders.

To be effective, these views on appropriate good practices should also be shared nationally, within all Member States.

REC81: NCCAs should set up one or more specific expert groups in charge of evaluating and sharing appropriate good practices, especially the ones on architecture and another pen testing or when the "state-of-the-art" is invoked. These expert groups should include all NCCA and major player in theses domains.

Justification: NCCAs should manage various national communities, through meetings, regular communications and publications, to share state-of-the-art and appropriate good practices. It should at least include all entities involved directly in the certification scheme (CAB, CSPs who have a service certification,). More specifically, good and appropriate practices should be shared and agreed between CABs and NCCAs, in order to ensure consistency of the evaluation, especially when it comes to domain that is strongly related to a highly volatile state-of-the-art (e.g. pentesting, evaluation of a secure architecture).

REC82: Besides managing communities of direct stakeholders, NCCAs should promote the cloud services certification through various communication operations, including the management of a community of national users of certified cloud service, on various topics (risk management, benefits of cloud certification…).

Justification: The scheme can flourish only if national users and stakeholders understand the benefits of a certification and are aware of some key points (e.g. specific attacks or technologies) and methodologies (e.g. risk management).

5.4 High

5.4.1 Introduction

The objective of the High level of assurance is to provide a certificate that ensures that the highest level of confidence, in a service that satisfies all the required organisational and technical security requirements, is achieved. The assurance level High is recommended for those services that are used within (highly) regulated industrial sectors such as Finance and Healthcare, highly critical business or/and highly sensitive information.

The process of achieving a High level of assurance is a combination of several components:

- A more stringent security measures requested when compared to the levels basic and substantial
- A more comprehensive and thorough audit and assessment approach, including pentesting and increased reassessment frequency (e.g. continuous auditing)
- A rigorous governance structure.

CSPCERT WG covered the security requirements in Annex 1 and section 4.4 of this document. The following section provides details about the assessments/audit approaches and the governance structures.

5.4.2 Auditing approaches

The auditing and assessment mechanisms related to the High level of assurance would need to ensure that a higher level of confidence is provided by:

- Increasing the frequency of the assessments, so to ensure that a certain security control objective is fulfilled at any given time and not only within a certain period of time. More specifically, that means moving from a 'point in time' or 'over a period of time' auditing approach, typical of auditing standards such as ISO/IEC 270xx or ISAE 3000 to continuous auditing-based certification approach.
- Adopting a more comprehensive and thorough audit approach that includes pentesting and vulnerability assessments to the process of evidence collection based on interviews, table top-exercises and analysis of the documentation.

5.4.2.1 Continuous Auditing

Continuous auditing is meant to improve the nature of auditing from a traditional, process-driven, point-in-time certification towards a data-driven real-time certification. The purpose of a certification based on a more frequent assessment of controls is to obtain an up-to-date verification that the control objectives and the technical control specifications are properly implemented by the CSP and that a certain level of assurance can be demonstrated at any given time.

A continuous auditing-based certification has to leverage, in addition to standard auditing mechanisms (e.g. analysis of policies, processes and procedures, technical documentation, etc), in technology that monitors and flags non-compliant activities in an ongoing basis. To this end, the assessment frequency via a continuous workflow needs to be increased. State-of-the-art security monitoring systems supervise the IT's security status by collecting data from the CSP's information system. This collected data is further assessed and used as the basis for continuous auditing.

A continuous auditing approach should be based on normalised data, making assessments unambiguous, repeatable and potentially comparable across different information systems. During the data normalisation process, security controls are translated into actionable security "measures", which describe constraints on security attributes of an information system. This process enables systematic and more frequent compliance checks.

REC83: It is recommended that ENISA assesses existing solutions for continuous auditing (like for instance the EC funded project EU-SEC [25]) to understand how that can be leveraged to increase the level of assurance provided at level high.

Justification: The use of continuous auditing approaches in the certification landscape is relatively new and not yet mature, nevertheless it represents a major advancement compared to existing assessment approaches based on "point-in-time" or "over-a-period-of-time" evaluation. Such an advancement is required to offer sufficient guarantees in highly critical areas like the cloud for the financial and healthcare sectors.

5.4.2.1 Penetration testing

CSPCERT WG has elaborated on the relevance of penetration testing in section 4.5 which is applicable to this section too.

5.4.3 Roles and Governance Specific to High

The governance structure shall ensure that all actors in the CSP Certification scheme:

1. Share the same level of information regarding threats and assessment methodologies;
2. Harmonize practices, e.g. agree on the technical level of the controls and the evaluation methodologies pertaining the certificate;
3. Agree on the equivalence between any newly adopted national NCCA scheme implemented to evaluate the CSP Services and existing recognized public certifications and
4. Deliver the corresponding certificate aligned with the CSP service certification scheme.

The governance structure described here deals with the suggested tasks, roles and relationships of the various stakeholders:

- Between the National Cybersecurity Certification Authority (NCCA), ENISA and various bodies at European level;
- Between the NCCA and different national stakeholders, at national level.

The following sections provide recommendations on the roles and relationships among the different entities involved in the certification scheme for the assurance level high. Moreover, some specific aspects, like peer review, are stressed in specific sections.

At national level, the organization of the CSP service certification scheme governance structure should be in line with the governance model shown below:

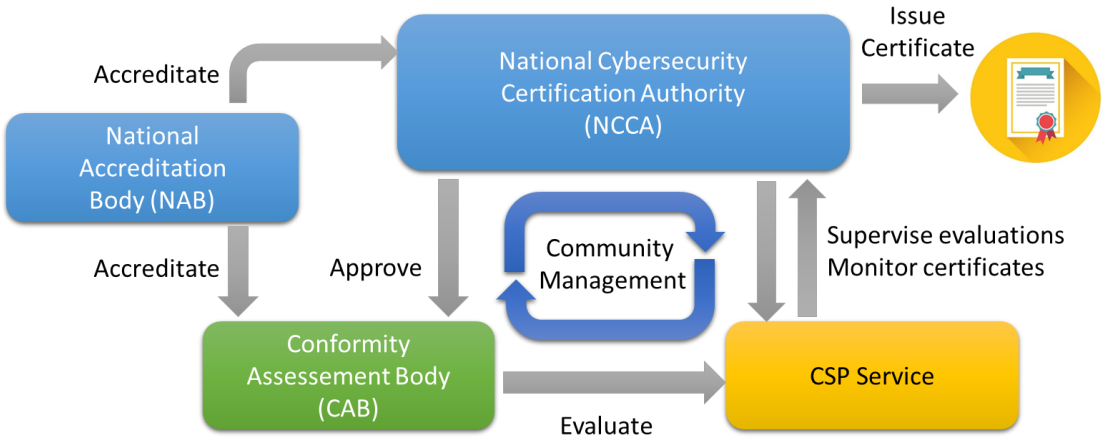

Figure 9. Governance structure - High.

Four entities are involved at this level:

1. *The National Cybersecurity Certification Authority (NCCA),* which executes, at national level, the decision of the Management Committee regarding the CSP service certification and manages the scheme at national level;
2. *The National Accreditation Body (NAB),* who is in charge of accrediting the conformity assessment bodies and the NCCAs, in order to be able to issue certificates;
3. One or many *Conformity Assessment Bodies,* who are in charge of performing the evaluations under the supervision of the NCCAs.

4. *Cloud Service providers,* applying to the certification process for one or many of their services.

For the assurance level high, according to the EUCA, the NCCA is responsible for issuing a mutually recognized certificate as well as of ensuring the proper recognition of the certificate.

REC84: The National Cybersecurity Certification Authority should:

1. Participate actively to the Management Committee at European level. Some of the expected activities include:

- To make proposals and comments regarding the strategies and governance of the managing committee;
- To make proposals and comments for decisions to be undertaken by the managing committee;
- To possibly participate in the Conciliation Commission, upon election and on a temporary basis;

2. Ensure that the technical skills and organization of the Conformity Assessment Bodies match the requirements for the assurance level high by:

- Performing periodical assessments of the technical skills of the evaluation from CABs;
- Approving formally the CABs, according to these technical assessments and a formal accreditation by the NABs.
- Developing communities and fora to share and harmonize critical evaluation practices (e.g. pentesting) among CABs;

3. Support the peer review process, especially by:

- Taking an active part in the evaluation process;
- Defining and agreeing within the Management Committee specific rules and controls pertaining to the peer review process;

4. Hold the responsibility for issuing the certificate for the high level, especially:

- Acknowledging and validating the auditing framework that will be used by the CABs to perform the evaluation of a CSP service;
- Supervising the evaluation tasks to be performed by the CABs;
- Validating the evaluation report and issuance of the certificate, based on that report;

5. Maintain, publish and transmit the following list to the ENISA:

- Up-to-date national list of approved Certification Assessment Bodies;
- Pp-to-date national list of certificates that are valid;

6. Monitor the issued certificate;

7. Report to the other NCCAs relevant incidents implying certified cloud services that could have an EU level impact;

8. Produce an annual document detailing the national activities performed towards the awareness of cloud services certification;

9. Manage a national community of stakeholders (CSPs, CABs, users), in order to promote and harmonize best practices regarding cloud cybersecurity.

Justification (1): At national level, the NCCA issues the certificate and is responsible for its consistency. Besides validating the evaluation report content to ensure its consistency, the NCCA needs to harmonize the evaluation practices. Consequently, at national level, each NCCA needs to manage the scheme and promote evaluation and security practices between all stakeholders.

Justification (2): The mutual acceptance of certificates is pertained at EU level by a mutual recognition and agreement between EU member states of how the scheme is managed nationally for each member state by including reference documentation used for the evaluation, methodology used, skills level of all the stakeholders at a national level. Thus, each member state has to build confidence and trust on how other member states manage nationally the same certification scheme. This can only be achieved by a consensus between all NCCAs on the reference framework controls and the assessment methodologies used, which should be maintained through time while providing a certain level of transparency. Accordingly, and more especially in the framework of the Management Committee, NCCA activities at EU level should support all the activities related to the maintenance and the management of the scheme.

The national accreditation body (NAB) is in charge of accrediting the conformity assessment body (CAB).

REC85: Consequently, the NAB should:

1. Comply with the REGULATION (EC) No 765/2008 [26], for accreditation and market surveillance relating to the marketing of cloud services and repealing Regulation;

2. Accredit the conformity assessment bodies against one or more specific methodologies for the evaluation of cloud services that:

- Are part of a standard/norm recognized by the Management Committee (e.g. ISO/IEC 17065 [19], ISO/IEC 17021 [17] or ISAE [27] [28]) and;
- Include the mandatory additional requirements identified by the Management Committee to ensure mutual recognition.

Justification: Relying on a mutually recognized accreditation schemes and standard evaluation methodologies (e.g. ISO/IEC 17065, ISAE...) puts a solid basis for mutual recognition of the issued certificates. Besides, gaps could exist between these standards. Additional requirements for the accreditation of the CABs could be identified and agreed by the Management Committee to fill them, which have to be assessed by the NABs.

REC86: In order to be allowed to perform the evaluation of cloud services, the conformity assessment bodies (CAB) should:

1. Be properly accredited by the NAB, against a norm or standard recognized by the Management Committee;

2. Be approved by the NCCA, to ensure the consistency;

3. Report its activities related to the cloud services certification;

4. Support the NCCA for the national maintenance of the cloud service certification scheme

Justification: The approval and the accreditation of the CAB ensures that their skills and methodologies are recognized at national level and endorsed by the NCCA that supervises and controls the scheme. As transparency is required, reporting actively activities to the NCCA helps to consolidate it at EU level.

For assurance level high, the NCCA issues the certificate based on the evaluation performed by the CAB, which means that the CAB must report on the evaluation to the NCCA and the decision on the certification is done by the NCCA, upon review of the evidence brought.

REC87: Consequently, the NCCA should be formally accredited by the NAB.

Justification: For issuing certificates, the NCCA needs to be accredited itself by the NAB (as required and according to the EUCA), under conditions that are similar to the ones of the CAB.

REC88: The CSP involved in the certification should:

1. Ensure actively after the certification that it still complies with the controls of the reference documents through an appropriate monitoring mechanism;
2. Report the NCCA any incident related to any of its certificated services;
3. Anticipate renewal of its certifications before they effectively expire.

Justification: The CSP's commitment is mandatory through the whole certification process, in order to ensure its success. Especially, requirements coming from the EUCA like vulnerability management and monitoring of the certificate implies a strong commitment of the CSP after the issuance of the certificate.

5.4.4 Transition from existing schemes

Where a CSP has obtained evidence derived from its adherence to an existing scheme (such as a certificate or audit report), this evidence may be presented by the CSP to the NCCA in order to issue the certification of its cloud service against this scheme.

However, the NCCA retains full freedom of appreciation in relation to this evidence, and the evidence has no particular status or binding force upon the NCCA nor the EU-wide Cloud certification scheme.

5.5 Substantial

5.5.1 Introduction

Demands to Substantial coming from the associated uses cases

As described in section 3.3.1, the substantial level aims for, e.g. "*business processes that are not high critical for the survival of an enterprise*" in various sectors, including the public sector. A high demand for CSP service certifications for the level substantial is expected. Therefore, the EU-wide certification

scheme should provide procedures that are easily rolled out and are "elastic" to respond to high demand. However, neither the security level nor the trust in the conformity assessment methodology should be substantially diminished. This can be achieved by reusing existing conformity assessment methods that are available in all EU member states.

REC89: The certification scheme should provide processes for certification that are easily rolled out and are "elastic" to respond on high demand.

Justification: High demand for certification for level substantial is expected.

In contrast to level high, the goal in substantial is not to achieve the highest possible level of confidence and technical level, but to set a solid and sufficient level of security to foster trust in certified CSP services and give the users a very high level of transparency.

REC90: The certification for level substantial should give the cloud user a high level of transparency concerning service delivery, security measures and outcome of the audit. The security of the CSP service should not be compromised in making this information available for customers.

Justification: Even though the CSP service certification shall be trusted, in many cases enterprises need to include cloud service into its risk management processes and therefore need transparency of the consumed cloud service.

Milestone 2 (located in Annex 2 of this document) includes an evaluation of the suitable conformity assessment methodologies to be considered within the context of EUCA. In particular, section 1.3. of Annex 2, summarises the fact that ISO-based and assurance-based (or ISAE-based) audits should be considered as viable options to satisfy the requirements of the three levels of assurance defined in EUCA (i.e. basic, substantial and high).

REC91: The CSPCERT WG recommends that in order to achieve a substantial level of assurance either an ISO-based certification or an ISAE-based attestation should be used.

Justification: To ensure a substantial level of assurance, the certification process has to be based on auditing standards that 1) guarantee a sufficient level of formality and rigor, 2) are based on a thorough assessment and standard, and repeatable processes, 3) offer accurate reporting standard, 4) there exist clear and well-defined auditor competences requirements, and finally that 5) have strong governance mechanisms in place to guarantee the sufficient level of oversight. Having these requirements in mind, ISO-based and ISAE-based auditing standards are considered to be the only suitable options currently available.

5.5.1.1 ISO-based audit

For further details on ISO-based audit please refer to Section 3 of Annex 2.

While ISO-based certifications (e.g. ISO/IEC 27001) represent a viable option for Substantial from an auditing standard perspective, it is important that the certification is based on a set of security requirements/control objectives which are cloud relevant (e.g. ISO/IEC 27017, ISO/IEC27018, BSI C5, the requirements of M1, etc).

REC92: The CSPCERT WG recommends that for ISO-based certifications to be accepted at Substantial level, the set of controls included in the statement of applicability are cloud relevant (e.g. ISO/IEC

27017, ISO/IEC27018, BSI C5, the requirements of Milestone 1, etc). Those cloud relevant controls should be added to the ones included in ISO/IEC 27002.

Justification: ISO/IEC 27001 is a useful certification to establish the security of an ISMS, but it does not necessarily guarantee an adequate coverage for cloud services unless additional cloud relevant control objectives are added to the auditing process.

5.5.1.2 ISAE-based audit

In this section, additional details about ISAE-based audits are provided. Those details will help to clarify the content included in Annex 2 - Section 4. ISAE 3000 and ISAE 3402 are widely used and proven trustworthy in industry, explicitly in the financial sector. The audit evaluates a given set of criteria (e.g. pre-defined control objectives and related measures) without exception. Audits according to ISAE 3000 are performed by public accountants with sufficient knowledge of the audit subject.

REC93: ISAE 3000 [27] and ISAE 3402 [28] auditing and reporting standards should be considered are suitable option for certifying CSPs service at assurance level substantial under the condition that the audit is performed by public accountants with sufficient knowledge of the matter.

Justification: The "ecosystem" of public accountants and ISAE fulfils REC82 and REC89. Public accountants need to comply with high standards (e.g. ethical, knowledge, objectivity). Moreover, public accountants are at a high degree liable (legally) for the correctness of the attestation they give. Finally, Public Accountants are located in all EU member states and many of them are able to operate multi-national that might be necessary to certify multinational CSP services.

Due to its nature as an attestation, it is not aligned with EUCA because it does not fit the definition of a certification. So, some additional efforts need to be undertaken to use a conformity assessment based on ISAE 3000 in CSP service certification framework for the level "Substantial".

REC94: The CSP service certification framework should neither alter, modify audit procedures nor report other rules of ISAE 3000 resp. ISAE 3402 in any way so that all criteria of ISAE are still fulfilled.

Justification: ISAE 3000 audits and ISAE 3402 reports have a value even if they are not used for a CSP service certification. The ISAE 3000 audit evidence can be the basis for different reports. This is a basis for efficient audits and so reducing effort and cost at the CSP. The CSP service certification should not have requirements that hinders efficient auditing and reuse of audit evidence.

REC95: Audit and report should be of a type 2 (see Annex 2 – section 4.2) because the effectiveness of the measures taken is of special interest and value in case of cloud services. For the first certification of a cloud service, audit and report could be of type 1 (without effectiveness).

Justification: Cloud services are constantly exposed to cyber threats and at the same time are updated nearly permanently. Therefore, a mere evaluation of the design of the cloud service does not meet the legitimate expectations and needs of the customers of the cloud service. Even more, it could leave the customer in a false persuasion of security.

REC96: The methodology of the conformity assessment based on ISAE 3000 and ISAE 3402 should be considered sufficient and for the certification no additional audit activities should be necessary.

Justification: Additional mandatory tasks in auditing or reporting that could not fit into ISAE 3000 and ISAE 3402 would lead to more complex audits and hinder the adoption of the CSP service certification.

Certification based on an ISAE3000 audit and ISAE 3402 report

The following additional requirements need to be fulfilled to issue certificates for the level substantial within the EU cybersecurity certification framework based on a conformity assessment according to ISAE 3000/3402 and performed by public accountants.

EUCA states (art. 56(4).) that for the level substantial, the Conformity Assessment Bodies that meet the requirements outlined in the Annex of the EUCA, issue certificates. The Conformity Assessment Bodies (CAB) must have the accreditation of the National Accreditation Body (NAB) (pursuant Regulation (EC) No 765/2008 [26]).

REC97: The Conformity Assessment Bodies (CABs) should meet all requirements to issue certificate aligned with ISO/IEC 17065. NCCAs could also act as a CAB undergoing the same procedure as a CAB.

Justification: ISO/IEC 17065 is the established international standard for certification of products, services and processes. ISO/IEC 17021, as a standard for management systems, does not fulfil the requirements of the EUCA unless extended as in REC92. Audit companies that issue attestations according to ISAE 3000 and ISAE 3402 could act as CAB, when requirements therefore are fulfilled, but is not in any way limited to.

5.5.2 Roles and Governance

For Substantial, the General Roles and Governance apply as provided in the Introduction to Section 5.5.

General remark:

For Substantial, not only NCCAs issue certificates but also CABs. To ensure consistency between certificates, the established rules in ISO/IEC 170xx and the governance of the scheme should be at EU level and not at national level.

Specific to Substantial is the ability of a NCCA to choose to approve a Conformity Assessment Body (CAB) to conduct an evaluation, which could include audit firms. Where that occurrence happens, the CAB conducts the evaluation, issues the certificate, and becomes responsible for the supervision and monitoring of the certificate. There are also instances, where the same body may elect to conduct those evaluations themselves and, thereby inherit the supervision and monitoring efforts.

This is illustrated in the following picture:

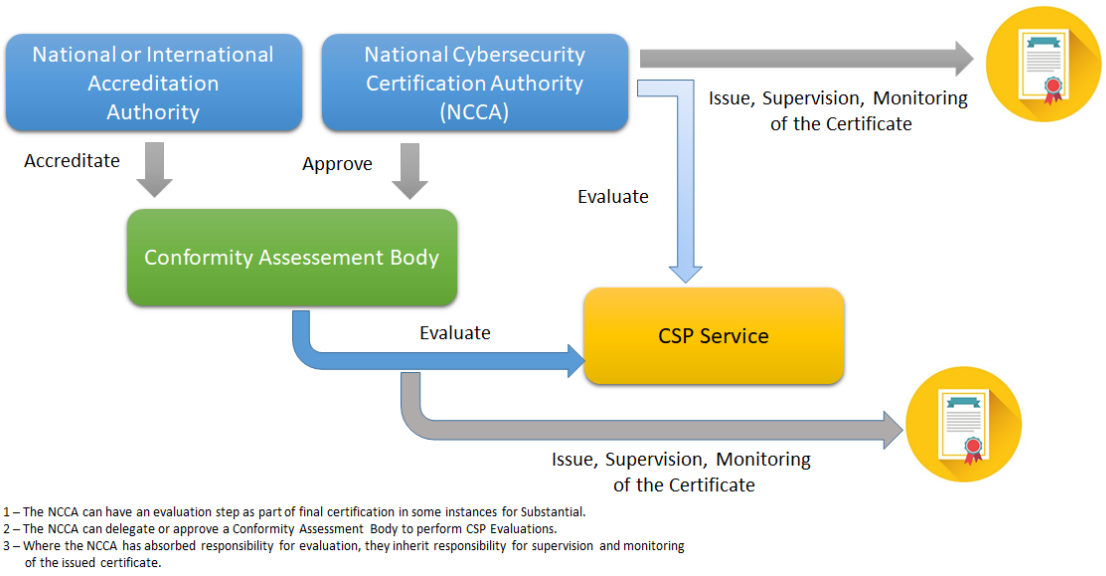

Figure 10. Governance structure - Substantial.

5.5.3 Transition from an Existing Scheme

Where a CSP has obtained evidence derived from its adherence to an existing scheme (such as a certificate or audit report), this evidence may be presented by the CSP to the NCCA or the CAB in order to issue the certification of its cloud service against this scheme.

However, the NCCA or CAB retains full freedom of appreciation in relation to this evidence, and the evidence has no particular status or binding force upon the NCCA or CAB nor the EU-wide CSP service certification scheme. ENISA could, as part of their final recommendation, build a certification scheme based on member states public certification schemes such as BSI C5 which would be recognized as the substantial level for the final scheme, and take on the maintenance of that framework within a final governance structure for the scheme.

5.5.4 Publicity and Promotion of Certificate

There is no unique requirement for Publicity and Promotion for Substantial.

5.5.5 Ongoing Maintenance and monitoring of assurance level

There is no unique requirement for this that has not already been described for the common framework in this document.

5.6 Basic

5.6.1 Introduction

In line with the requirements of the EUCA, a 'basic' level certification 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*".

As it was already explained in section 3.3.2 above, the current proposal builds on the perspective that the security objectives and controls should be identical for all three levels of assurance in the present scheme, and that the principal distinction lies on the depth of verification applied to the controls. The CSP service certification under this scheme is therefore based on the strict conformance to a predefined list of controls, which are common among all three levels of assurance.

Even at the basic level, the EUCA requires 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. On this basis and taking into account the technical complexity of cloud computing, this scheme does not allow unverified statements of conformity self-assessment under the sole responsibility of the CSP, even at the basic level of assurance. While the CSP should indeed be required to conduct the necessary initial verification of compliance with the objectives and controls of this scheme, even at the basic level there will be a verification by a neutral (or independent) third party - the Monitoring Body - of the documentation created or compiled by the CSP as a part of its internal verifications. Provided that the Monitoring Body approves, the CSP should thereafter receive a certificate from the NCCA. Thus, no EU statement of conformity in the sense of the EUCA is supported by this scheme. This approach has been referred to in the recommendations above as an ‘’evidence-based conformity assessment’.

Recommendation 30 (literally) and 82, 89 (accordingly) apply to the basic level

5.6.2 Roles and governance

For the assurance level ‘basic’, the General Roles and Governance largely apply as provided in the Introduction to Section 5. There are however a few small required modifications, notably:

- The role of the CSP is expanded, as it will conduct the initial evaluation of compliance itself and will establish appropriate documentary evidence to allow third party verification of its compliance.
- The role of the Monitoring Body is modified and to some extent, simplified:
    - Rather than conducting a comprehensive evaluation of the CSP Service, the Monitoring Body evaluates the provided documentary evidence in order to determine whether (1) the evidence addresses the security requirements of the scheme in a sufficiently comprehensive manner; (2) the evidence is sufficiently clear and unambiguous in how the requirements are met and how controls have been implemented by the CSP; (3) the evidence is *prima facie* plausible (i.e. it appears in the professional opinion of the Monitoring Body that there are no elements in the evidence that are manifestly inaccurate, incomplete or false) and verifiable (it can in principle be verified by an on-site audit).
    - As a part of the submission of the evidence to the Monitoring Body, the CSP must authorise the Monitoring Body to conduct an on-site inspection at the CSP’s premises and of the CSP’s facilities used as a part of the Service, whenever the Monitoring Body has received a complaint or has other reasons to conduct additional verifications.
    - The Monitoring Body assumes no responsibility through this checking process for the content or accuracy of the evidence. The Monitoring Body must obtain an unambiguous and binding statement from the CSP that the evidence provided is accurate, up to date, not misleading, and that the CSP has not knowingly omitted elements that it knew or should have known would affect the compliance to the security objectives and thus the evaluation by the Monitoring Body. The cloud service

provider assumes full responsibility for the compliance of the cloud service with the legal requirements of the European cybersecurity certification scheme.

- After the Monitoring Body confirms that the evidence satisfies the requirements of assurance level basic, a report of the evaluation is sent to the NCCA, which will decide if a certificate can be issued, based on the report and on any other elements that the NCCA deems relevant.
- Given that the approach is evidence-based with evidence provided by the CSP, the Monitoring Body should in principle not:
  - Conduct a review of the (non-)applicability of publicly known vulnerabilities
  - Conduct a review of the correct implementation of the necessary security functions
  - Assess the CSP Service's resistance to skilled attackers via penetration testing
  - However, as noted above, the Monitoring Body should have the right to conduct on-site audits whenever the Monitoring Body has received a complaint or has other reasons to conduct additional verifications; such on-site audits may include all elements listed above

- Other elements remain as provided in the Introduction to Section 5, including with respect to the appointment of the Monitoring Bodies by the NCCA, their periodic surveillance by the NCCA, and their adherence to a uniform scheme of requirements. The responsibility for the surveillance of the Monitoring Body lies with the NCCA which will ensure that the technical skills and organization of Conformity Assessment Bodies match the requirements and that the assessments are performed according to a consistent standard. This inspection should be performed regularly on an annual basis.
- The Monitoring Bodies shall adhere to the requirements set out in the Annex of the EUCA regarding competence and independence

This is shown in the figure below:

Figure 11. Governance structure - Basic.

REC98: Monitoring Bodies should be appointed by the NCCA based on uniform criteria and should act based on a uniform process manual.

Justification: In principle the competence and independence of the monitoring bodies and the method of assessment should not vary.

5.6.3 Transition from existing scheme

No particular recommendations apply. Where a CSP has obtained evidence derived from its adherence to an existing scheme (such as a certificate or audit report), this evidence may be presented by the CSP to the Monitoring Body. However, the Monitoring Body retains full freedom of appreciation in relation to this evidence, and the evidence has no particular status or binding force upon the Monitoring Body.

5.6.4 Ongoing Maintenance and monitoring of assurance level

No particular recommendations apply. However, as the evidence on which the certification is based is created or compiled by the CSP, the CSP shall be required to provide updated relevant information to the applicable Monitoring Body when the evidence is no longer in line with reality in a manner which would require re-evaluation by the Monitoring Body.

References

[1] ENISA, “Cloud Certification Schemes Metaframework,” 2014. [Online]. Available: https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework. [Accessed October 2018].

[2] L. Orue-Echevarria, C. Cortés, M. Alvarez, B. Sanchez and A. Ayerbe, “Certification schemes for cloud computing,” EU Publications office, Luxembourg, 2019.

[3] ANSSI, “Extract from Cloud IT service providers (SecNumCloud) – Requirements Reference Document – Essential level. Version 3.0,” 2017.

[4] BSI - German Federal Office for Information Security;, “Cloud Computing Compliance Controls Catalogue (C5),” 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf.

[5] ISO / IEC, “ISO/IEC 27002:2013: Information technology -- Security techniques -- Code of practice for information security controls,” 2013.

[6] ISO / IEC, “ISO/IEC 27017: 2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services”.

[7] ISO / IEC, “ISO / IEC 27018: 2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”.

[8] Cloud Security Alliance, “Cloud Controls Matrix v3.0,” [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwijz6uMmNLiAhVy8OAKHQhkDH4QFjACegQIAhAC&url=https%3A%2F%2Fdownloads.cloudsecurityalliance.org%2Fassets%2Fresearch%2Fcloud-controls-matrix%2FCSA_CCM_v.3.0.1-06-06-2016.xlsx&usg=AOvVa. [Accessed 2018].

[9] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations - NIST Special Publication 800-53. rev 4,” 2014.

[10] ANSSI, “SecNumCloud – La nouvelle référence pour les prestataires d’informatique en nuage de confiance,” ANSSI, 2018. [Online]. Available: https://www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/. [Accessed May 2019].

[11] NIST, “Security and Privacy Controls forFederal Information Systems and Organizations,” 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4. [Accessed 2019].

[12] ISO/IEC, “ISO /IEC 27002: 2013 - Information technology - Security techniques - Code of practice for information security management”.

[13] ISO, “ISO/IEC 19086-4:2019: Cloud computing - Service level agreement (SLA) framework -- Part 4: Components of security and of protection of PII,” 2019. [Online]. Available: https://www.iso.org/standard/68242.html .

[14] ISO, "ISO 31000:2018(en): Risk management — Guidelines," 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. [Accessed 2019].

[15] European Parliament;, "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. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN. [Accessed 2019].

[16] Government of Spain;, "Spain: National security scheme - ENS," 2019. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/en/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html?idioma=en#.XO-b5ogzbD5. [Accessed 2019].

[17] ISO / IEC, "ISO/IEC 17021: Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements," 2015. [Online]. Available: https://www.iso.org/standard/61651.html. [Accessed 2019].

[18] ISO / IEC, "ISO/IEC 17065: Conformity assessment — Requirements for bodies certifying products, processes and services," 2012. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso-iec:17065:ed-1:v1:en. [Accessed 2019].

[19] ISO / IEC, "ISO/IEC 17065:2012 - Conformity assessment -- Requirements for bodies certifying products, processes and services," 2012. [Online]. Available: https://www.iso.org/standard/46568.html. [Accessed 2019].

[20] ISO / IEC, "ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements," 2013. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed 2019].

[21] Eurocloud, "Eurocloud Star Audit," [Online]. Available: https://staraudit.org/. [Accessed 2019].

[22] LEET, "LEET Security," [Online]. Available: https://www.leetsecurity.com/. [Accessed 2019].

[23] Cloud Security Alliance, "CSA Security Trust Assurance and Risk (STAR) Program," [Online]. Available: https://cloudsecurityalliance.org/star/#_overview. [Accessed 2019].

[24] Zeker, "Zeker Online," [Online]. Available: https://www.zeker-online.nl/. [Accessed 2019].

[25] EU-SEC Consortium;, "Continuous Auditing Based Certification," [Online]. Available: https://www.sec-cert.eu/eu-sec/Continuous_Auditing_Certification. [Accessed May 2019].

[26] European Parliament, "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 ofproducts and repealing Regulation (EEC) No 339/93," 0208. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0765&from=ES. [Accessed 2019].

[27] International Standard on Assurance Engagements;, "INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS 3000 - ASSURANCE ENGAGEMENTS OTHER THAN AUDITS OR REVIEWS OF HISTORICAL FINANCIAL INFORMATION".

[28] International Auditing and Assurance Standards Board (IAASB);, "AUDITING INTERNATIONAL STANDARD ON ASSURANCE ENGAGEMENTS (ISAE) 3402: ASSURANCE REPORTS ON CONTROLS AT A SERVICE ORGANIZATION".

[29] PCI Security Standards Council;, " Payment Card Industry Data Security Standard," [Online]. Available: https://www.pcisecuritystandards.org/document_library#agreement. [Accessed 2019].

[30] European Commission;, "COM(2017) 477 final – Proposal for a regulation of the European parliament and of the Council on ENISA, the "EU Cybersecurity agency" and repealing regulation (EU)526/2013, and on Information and Communication Technology cybersecurity certification ("Cybe," 2017.

[31] ISO / IEC, "ISO/IEC 17000:2004 – Conformity assessment – Vocabulary and general principles," 2004.

[32] ISO, "ISO 19011:2018 – Guidelines for auditing management systems," 2018.

[33] European Parliament, "European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communicatio," 2019. [Online]. Available: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#title2. [Accessed 2019].

[34] European Parliament, "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=ES. [Accessed 2019].

[35] European Parliament, "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, 200," 2012. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=EN. [Accessed 2019].

[36] American Accounting Association - Committee on Basic Auditing Concepts;, A Statement of Basic Auditing Concepts, Sarasota, US: American Accounting Association, 1973.

[37] ISO, "ISO/IEC 27000:2018 - Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[38] NIST, "The NIST Definition of Cloud Computing - NIST Special Publication 800-145," 2011.

[39] European Commission, "COM(2012) 529 final. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Unleashing the Potential of Cloud Computing in Europe," 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

[40] ISO, “ISO/IEC 17789:2014 - Information technology -- Cloud computing -- Reference architecture,” 2014.

[41] ISO, “ISO/IEC 19086-1:2016 - Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts,” 2016.

[42] ISO, “ISO/IEC 17788:2014 - Information technology -- Cloud computing -- Overview and vocabulary,” 2014.

[43] European Commission, “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,” 2016.

[44] ISO, “ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements,” 2013.

[45] ISO, “ISO/IEC 19941:2017 - Information technology -- Cloud computing -- Interoperability and portability,” 2017.

[46] NIST, “Guide to Information Technology Security Services - Special Publication 800-35,” 2003.

[47] ISO, “ISO/IEC 29100:2011 - Information technology -- Security techniques -- Privacy framework,” 2017.

[48] NIST, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations - SP 800-162,” 2014.

Annex 1 – Milestone 1: Security objectives

1 Introduction

1.1 About this annex

The aim of this annex is threefold. Firstly, it presents the methodology followed by the CSPCERT WG view to elicit the security objectives or requirements that an EU-wide cloud security certification scheme should cover. Secondly, it presents the elicited security objectives. Thirdly, it presents the high-level gap analysis between the following schemes: ISO/IEC 27002 [5], ISO/IEC 27017 [6], ISO/IEC 27018 [7], ANSSI SecNumCloud [3], BSI C5 [4], ENISA Cloud Computing Schemes Metaframework [1]. The previous standards and certifications were selected based on the objectives of the Cybersecurity act that targets existing European public certifications and the inclusion of ISO as a standard to be used.

This annex was released as a stand-alone document and made available to the public during the period of the open consultation. Several comments and considerations were received and have been incorporated as agreed by the CSPCERT WG.

1.2 Annex structure

The rest of this annex is structured as follows:

- Section 2 describes the methodology followed to extract the security objectives, that can also be used for requirements that can arise in the future,
- Section 3 describes the security requirements,
- Annex 1a contains the high-level gap analysis. This is done this way to ensure a better legibility of the document.

2 Methodology

The methodology followed for the definition of the security objectives is detailed below.

The following documents have been used as input sources:

- Study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [2]
- ISO 27002 [5], 27017 [6], 27018 [7]
- ENISA Cloud Computing Schemes Metaframework (CCSM) [1]
- BSI C5 [4]
- SecNumCloud [3]

During the open consultation, respondents were asked about the adequacy of including further schemes in the analysis such as PCI-DSS [29], Cloud Security Alliance Cloud Control Matrix (CSA CCM) [8], NIST 800 - 53 [11] or any other relevant one that the respondent felt appropriate. While CSA Cloud Control Matrix, SOC2 and PCI-DSS were suggested by many respondents, the following considerations were taken into account:

- Based on the results of previous studies, e.g. [2] on [1] the gaps between the CCM requirements and those included in any of the other control frameworks considered in this analysis (and vice versa) are rather small; for instance the BSI C5 controls are based on the controls of the CSA Cloud Control Matrix in a large proportion; therefore the CCM fully satisfies the security objectives defined in Chapter 3 of this document.
- PCI-DSS [29] is different and could require a further assessment. PCI-DSS has different goals than the other schemes analysed, as it is aimed at a different constituency, so an EU level scheme is not likely to replace it.
- NIST 800 – 53 [11] has a very large number of controls. The mapping analysis available in study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [11] leads to think that the number of additional security objectives that could be derived is rather small.

A detailed mapping analysis which includes CSA CCM and NIST 800-53 is available in the study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [2], which can be checked at any time.

The methodology to extract the security objectives is described next. First of all, the above-mentioned schemes and relevant standards (ISO 27002, ISO 27017, ISO 27018, BSI C5 and SecNum cloud), taking as baseline ENISA CCSM have been analysed to seek for commonalities and families of controls. In this context, a 'family of controls', namely a domain, is a set of controls focused on a certain aspect, such as network security, operational security, or personnel. For simplification purposes, a family of controls is named as category (labelled as 'EC_Cloudcategory' in the spreadsheet that can be found in Annex 1a).

The categories of security objectives are identified are as follows:

1. **Information Security Policies:** ensure the definition of policies related to information security, aligned with the relevant laws, regulations, as well as with the business requirements of the organization. It also includes the definition of the appropriate roles and responsibilities to carry out the implementation of said policies.

2. **Personnel & Training:** Ensure that the employees and contractors are aware and understand their responsibilities towards the information security policies defined and implemented in the organization.
3. **Asset Management:** provide mechanisms for the identification and protection of organizational and information assets, also those coming from customers.
4. **Identity and Access Management:** Put in place the mechanisms to ensure the access to the information, information processing facilities and virtualized environments of only authorized users.
5. **Cryptography and Key management:** Ensure a secure operation of the cloud services with the definition and implementation of the appropriate cryptographic mechanisms.
6. **Physical Infrastructure Security:** Ensure the prevention of unauthorized access to the physical site so as to prevent any damage, loss, failure or theft of any of the business' assets that may hamper the organization's operations.
7. **Operational Security:** Ensure the secure and proper operation of the information security facilities so that the cloud service provider is always operational.
8. **Communications Security:** Ensure the protection of the information in networks, external and internal and in between systems.
9. **Procurement Management:** Define and implement mechanisms to manage the whole supply chain of the cloud service provider and ensure that these procurement activities maintain the appropriate security level.
10. **Incident Management:** Provide the means to manage, react to, and communicate security incidents.
11. **Business Continuity and disaster recovery**: Set out the activities needed to ensure the continuity of the operations of the cloud service recovery, including the disaster recovery ones while ensuring the integrity of the information at all times.
12. **Compliance**: Satisfy the legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
13. **Security Assessment:** To establish and maintain appropriate procedures for testing key network and information systems underpinning the cloud services and to establish and maintain appropriate procedures to perform security assessments of critical assets.
14. **Interoperability and Portability**: Provide means that allow customers to interface with other cloud services and/or if needed port to other providers offering similar services in a secure way.
15. **System Security and Integrity**: Put in place the appropriate measures to ensure that the system maintains an adequate level of security and integrity in its entire lifecycle, from development to operation, from internal developments to outsourced ones, using both commercial and open source software.
16. **Change and Configuration Management:** Establish and maintain change management procedures for network and information systems.
17. **Risk Management:** Provide the means to ensure an appropriate governance and risk management framework, as well as mechanisms to identify and address risks for the security of the cloud services

The second step has been the 1:1 matching of the controls of the selected certification schemes (ISO 27002, ISO 27017, ISO 27018, SecNumCloud, BSI C5 with ENISA CCSM as baseline) in each of the categories with the aim of analysing the differences, that is, the gap among of the existing schemes. It

is important to note that while a control could be matched to several categories, this has been placed in the category that was most substantively fulfilled. The starting point for this gap analysis was the study SMART 2016 / 0029 and incremented with ISO 27017, ISO 27018 and SecNumCloud. The complete final mapping can be seen in Annex 1.

	A	B	C	E	G
1	**EC-CLOUD CATEGORY**	**CCSM-ENISA**	**C5 GERMANY**	**SecNum FRANCE**	**ISO 27002**
3	Information Security Policies	CCSM-ENISA SO 01 - Information security policy CCSM-ENISA SO 03 - Security roles	C5 OIS-01 Information security management system (ISMS) C5 SA-01 Documentation, communication and provision of policies and instructions C5 SA-02 Review and approval of policies and instructions C5 SA-03 Deviations from existing policies and instructions C5 OIS-03 Authorities and responsibilities s in the framework of information security C5 OIS-04 Separation of functions C5 OIS-05 Contact with relevant government agencies and interest groups C5 OIS-06 Policy for the organization of the risk management C5 OIS-02 Strategic targets regarding information security and responsibility of the top management C5 OIS-07 Identification, analysis, assessment and handling of risks	SecNum 5.1. Principles SecNum 5.2. Information security policy **SecNum 6.1. Functions and responsibilities linked to information security** **SecNum 6.2. Segregation of tasks** SecNum 6.3. Relations with the authorities SecNum 6.4. Relations with specialised work groups SecNum 6.5. Information security in project management HYG33: Adopt security policies dedicated to mobile devices	ISO 27002: 5.1.1 A set of policies for informat defined, approved by management, published employees and relevant external parties. ISO 27002: 5.1.2 The policies for information review at planned intervals or if significant cha their continuing suitability, adequacy and effec ISO 27002: 6.1.1 All information security resp defined and allocated. ISO 27002: 6.1.2 Conflicting duties and areas should be segregated to reduce opportunities unintentional modification or misuse of the org ISO 27002: 6.1.3 Appropriate contacts with r should be maintained. ISO 27002: 6.1.4 Appropriate contacts with s or other specialist security forums and profes should be maintained. ISO 27002: 6.1.5 Information security should project management, regardless of the type o ISO 27002: 6.2.1 A policy and supporting sec

Figure 12. High level gap analysis (mapping) – Excerpt.

The third step is the derivation of the security objectives that the EU-wide security certification scheme should cover. To this end, based on the map and gap analysis performed in the previous step, an in-depth analysis has been carried out and the security objectives have been extracted. The document distinguishes between high-level and detailed objectives. While the high-level is the overarching goal of the objective, the detailed objectives present more information of the different aspects that need to be fulfilled.

New security objectives can come into place as the technology progresses, new schemes are to be incorporated, or as new sectors decide to include their own requirements in the EU-wide certification scheme. To this end, the current design allows for that. The process would be similar: identify under which category or categories the objective would fit in, analyse the delta and define the security control in case it is not yet under consideration.

In addition, current objectives may change. While for the time being, the version number of the objectives is not kept, this could be a field that could be added.

3 Security objectives

3.1 Information Security Policies

3.1.1 High level security objective

The Cloud Service Provider (CSP) must define, institutionalize and communicate, to internal and external stakeholders, the security policies, which must be approved by the top management. Roles and responsibilities related to such security policies must also be defined, assigned and communicated, also to internal and external stakeholders.

3.1.2 Detailed security objectives

ISP.1: The CSP must define and implement its information security policies. A well-defined information security policy shall include, among other aspects, baseline information security objectives, how these will be enforced, measured and its correctness evaluated so that appropriate corrective actions can be applied, threats as well as the policy sources (e.g. regulations, legislation, corporate strategy).

ISP.2: The CSP must complement the baseline information security policies with procedures related, among others, to the provisioning and usage of the cloud service, isolation, multi-tenancy, access rights, lifecycle management of a cloud service offering, lifecycle management of an account of a cloud service customer, compliance with applicable PII protection legislation, contractual agreements

ISP.3: The CSP must communicate all information security policies to both its internal and external stakeholders (e.g. cloud service customers).

ISP.4: The CSP must define, document and assign roles and responsibilities in the security policy, both at the cloud service provider's side and at the cloud customer's side, taking into consideration that:

a) The separation of roles and responsibilities must be ensured, so that operational and controlling functions are not performed by the same person at the same time. In the case it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be put in place.
b) Responsibilities for the protection of individual assets, for activities related to risk management and more specifically for the acceptance of residual risks, as well as for the implementation of certain security processes must be identified and defined.
c) No one can access, modify or use any asset without the proper authorization.
d) The cloud service customer data and applications custodied by the CSP must be considered for the allocation of roles and responsibilities.
e) Authorization levels must be identified and documented.

ISP.5: The CSP must communicate to all stakeholders, internal and external, any change occurred related to roles, responsibilities or contractual issues.

ISP.6: The CSP must document and implement the procedures that will have to be followed to report the corresponding authorities in a timely manner whenever a security incident has occurred.

ISP.7: The CSP must specify a point of contact regarding the processing of PII.

ISP.8: The CSP should maintain appropriate contacts with special interest groups, security fora, professional associations in order to improve the cooperation and coordination of security related aspects.

3.2 Personnel & Training

3.2.1 High level security objective

The CSP must ensure that employees and contractors are aware of, understand, and fulfil the information security responsibilities in the role for which they are considered, with the aim of protecting the organization's interests.

3.2.2 Detailed security objectives

PT.1: Prior to the employment contract, the cloud service provider must screen the background of the employee following a defined screening process and in accordance to the applicable laws and regulations. The background checks should be proportional to the business context, the sensitivity of the information that will be accessed by the employee and the associated risks.

PT.2: The contracts between employees and the CSP must state their role and responsibilities regarding the information security. Furthermore, the organization's policies in security matters such as access, confidentiality, ethics, management of the information and so on should be stated on the contract. A document containing the rules of behaviour with respect to how to deal with the information and data of the customers should be provided.

PT.3: The CSP as well as its external contractors and suppliers must make mandatory and available to all its employees a training programme in security such as information security in general (e.g. how to handle cloud data, threats, secure operation and management of data and information) and in security requirements. This training programme is to be tailored to the role and responsibility of each employee. Awareness raising campaigns and activities should be launched as a complement to the training programme.

PT.4: All CSPs employees and contractors must attend to the information security principles defined in accordance to the organization's policies and processes. This should also be abided and monitored by the management.

PT.5: The CSP must have a disciplinary process define and communicated. This process shall be put in place against employees who have committed an information security breach.

PT.6; The CSP must inform internal and external employees that the security responsibilities and requirements remain valid even if there is a contract termination or a change in the role. The terminated employee will also be informed with the need to comply with the relevant legislation, regulations regarding information security whenever this situation occurs.

3.3 Asset[4] Management

3.3.1 High level security objective

The CSP keeps and achieves appropriate protection of all organizational and information assets, including those originating from the customers.

3.3.2 Detailed security objectives

AM.1: The CSP must define, establish, manage and update an inventory of assets associated with information and which are necessary for information processing.

AM.2: The CSP must assign roles and responsibilities for the ownership of the assets.

AM.3: The CSP must define, document, implement, put in place and monitor the rules to handle assets, including bringing in and returning assets by customers.

AM.4: The CSP must establish and maintain a classification of the information assets along with an appropriate labelling and handling mechanisms.

AM.5: The CSP must define, document, implement, and monitor procedures for the secure handling, transfer and disposal of media of any kind.

AM.6: The CSP must define, document, implement, and monitor procedures for the secure handling of physical assets of a customer (e.g. hard drives, hardware security module (HSM)). These procedures must be communicated to the customer.

3.4 Identity and Access Management

3.4.1 High level security objective

The CSP must secure the authorization and authentication of its own users as well as those coming from the cloud service customer in order to prevent unauthorized access and mitigate cyber security risks derived from the use of virtual environments.

[4] In ISO/IEC 27000:2009 asset was defined as “anything that has value to the organization”, including: a) information (2.18); b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.

In ISO/IEC 27000:2014 the definition of asset was removed from the standard but still, the term “asset” is used, but mostly in the sense of an “information asset”.

In 2014, ISO published “ISO 55000:2014 - Asset management — Overview, principles and terminology” where asset is defined as “item, thing or entity that has potential or actual value to an organization”. (Note 1 to entry: Value can be tangible or intangible, financial or non-financial, and includes consideration of risks (3.1.21) and liabilities. It can be positive or negative at different stages of the asset life (3.2.2).

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.

Note 3 to entry: A grouping of assets referred to as an asset system (3.2.5) could also be considered as an asset.)

3.4.2 Detailed security objectives

IAM.1: The CSP must restrict access both to the stored information and to the facilities where the information is located. To this end, an access control policy should be defined, documented and implemented aligned with the organization's information security requirements.

IAM.2: The CSP must define, document and implement a user access management procedure, which shall include, among other aspects, a policy for providing and revoking permissions and privileges, a definition of the different access levels to read, write and delete information, policies to safeguard the non-disclosure of authentication and other sensitive information, and regular reviews.

IAM.3: The CSP must define and communicate to the whole organization the practices that must be followed in relation to the use of secret authentication information[5].

IAM.4: The CSP must define, document, implement, monitor and manage mechanisms such as multi-factor authentication, to prevent unauthorized access to virtualized environments, information systems, data and applications.

IAM.5: The CSP must define, document, implement, monitor and manage mechanisms to protect the separation of concerns in virtual environments, including customer data, applications, storage among others. This separation of concerns must include on one hand, the resources used by the cloud service customers through the CSP's offerings, and on the other hand, the administrative infrastructure that the CSP needs to run its business, which should not be in contact with the customers' used and offered resources.

3.5 Cryptography and Key management

3.5.1 High level security objective

The CSP must define, select, dimension and implement appropriate cryptographic mechanisms supported by an adequate key management infrastructure, in order to ensure a secure operation of its cloud services.

The use of cryptography should be mandatory for the CSP in order to ensure the security of information (confidentiality, authenticity and integrity). That concerns data at rest as well as data flows.

3.5.2 Detailed security objectives

CKM.1: the CSP must define, implement and use appropriate cryptographic and protocol standards in order to provide efficient robustness against threats like crypto analysis. This implies that:

i) Proper authentication protocol and mechanisms must be implemented for entities and user request access to or transacting with cloud's equipment and resources.
ii) When appropriate or required by regulation, proper digital signature mechanisms must be used in order to ensure authenticity of electronic assets or transactions.

CKM.2: The CSP must protect properly with appropriate cryptographic mechanisms and protocols all data flows that are exposed to public networks or other customers.

[5] Secret information: passwords, single sign-on procedures (SSO)

CKM.3: The CSP must protect with appropriate cryptographic mechanisms the cloud customer's and sensitive data, which could be exposed during maintenance, transport, reallocation or disposal of media or equipment. As an example, only the hash values of the passwords of the users and of technical accounts should be stored.

CKM.4: All cryptographic mechanisms operated by the CSP shall be supported by a proper key management infrastructure and key management policy.

3.6 Physical Infrastructure Security

3.6.1 High level security objective

The CSP must provide means to prevent unauthorized access to its physical site as well as protection against theft, damage, loss and failure of assets in order to ensure a continuous operation.

3.6.2 Detailed security objectives

PI.1: The CSP must put in place physical perimeter protection in defined public, private and sensitive areas.

PI.2: The CSP must limit the access to private and sensitive areas only to authorized personnel.

PI.3: The CSP must maintain the needed infrastructure and devices to ensure the availability and the integrity of the information.

PI.4: The CSP must define and put in place the measures needed to protect the infrastructure from outside and environmental threats, and against the disruption of base services such as electric power.

3.7 Operational Security

3.7.1 High level security objective

The CSP must manage, define, document, implement, monitor and evaluate procedures related to its operation such as different environments needed, capacities, resources, information, data, protection of facilities, (user and system) activities, safeguards, incidents, failures, among others.

3.7.2 Detailed security objectives

OS.1: The CSP must define, document, communicate and distribute all operation procedures and the associated roles and responsibilities in a written form to all users and stakeholders that need to make use of them.

OS.2: The CSP must define, implement and maintain a segregation of environments (e.g. development, testing and operation) in order to diminish the risk of unauthorized access as well as changes that can occur to the environment in production. To this end, the following aspects should be planned and implemented: procedures and conditions to transfer software from one environment to the others (e.g. when a software is promoted to production environment and under which criterion, how testing is performed in each of the environments, roles and permissions of the users for all environments, and so on).

OS.3: The CSP must plan and control capacities and resources (personnel and cloud resources). The planning should include forecasts to avoid, for instance, bottlenecks, overloads and other restrictions

to be able to comply always with the agreed service level agreements (SLAs). For the monitoring aspect, safeguards should be implemented that should control that the provision of cloud resources is ensured under the agreed contractual agreements.

OS.4: The CSP must ensure that the information, data as well as the information facilities are protected against malware and malicious code. For that, the defined procedures should include the implementation of controls for malware prevention and detection, installation of patches, user awareness activities, regular reports that could be audited anytime, authorization levels to the different data and information hosted, and protective measures for data coming from external sources, among others.

OS.5: The CSP must plan, implement and test a backup procedure in agreement with a backup policy to ensure that no information is lost and that it can be restored at any time. The backup policy should define the retention and protection requirements as well as other aspects such as frequency of backups, location of where they are being performed, extent (incremental or full), restoration procedure, and access authorization.

OS.6: The CSP must record user activities, system activities, failures, information security events, files accessed, user privileges, alarms raised, among other aspects, in logging facilities of the CSP. The log information stored should be protected from manipulation and unauthorized access. In order to ensure the synchronization of all these items, the CSP will have the clock synchronized to a single reference time source. The timestamp of this clock should be visible in the log files so as to be able to correlate and analyse the different occurred events.

OS.7: The CSP must define, document, implement and control a process to manage vulnerabilities. To this end, specific information such as the assets of the company, the software provider, their versions, the deployment status of the software, responsible people, and the risks among other should be recorded in different sources, namely logs.

OS.8 In order to maximize business continuity and therefore minimize disruptions, audit activities related to the evaluation of operational systems must be planned. The scope of the tests and the time in which they will be carried out need to be established and agreed. As a recommendation, they could be performed outside business hours.

3.8 Communications Security

3.8.1 High level security objective

The CSP must ensure an appropriate protection of communications in the networks, internal and external, and in between systems processing information.

3.8.2 Detailed security objectives

CS.1: The CSP must segregate the communications. The different parts of the network must be partitioned according to:

- the sensitivity of the information sent;
- the nature of the data flows (production, administration, supervision, etc.);
- the area that the data flows belong to (clients – with a distinction per client or set of clients, the service provider, third parties, etc.);

- the technical area (processing, storage, etc.);

in order to be able to apply the appropriate security measures on each partition.

CS.2: The CSP must define, document and regularly update and maintain a map of the information system and the network.

CS.3: The CSP must segregate the administration network from other networks (e.g. customers).

CS.4: The CSP must define, document, implement and monitor mechanisms, such as state-of-the-art cryptographic standards (SSL/TLS) and their countermeasures, to protect the communication flows from and to the cloud infrastructure, between infrastructures, as well as between customers and infrastructures.

CS.5: The CSP must monitor, according to the regulations (e.g. like lawful interception) the communication flows within the cloud, internal and external, to respond appropriately and timely to threats.

3.9 Procurement Management (Supply chain management)

3.9.1 High level security objective

The CSP must establish, implement and maintain security procedures, policies and associated security requirements to manage its suppliers, in order to ensure that such procurement and outsource do not affect the security level of the cloud services. The CSP must ensure that these policies are also kept in its supply chain.

3.9.2 Detailed security objectives

PM.1: The CSPs must define, implement and maintain a procurement management procedure that defines the principles that ensure that security is part of the procurement process, including outsourced development and supporting utilities.

PM.2: The CSP must define, implement and maintain the mechanisms to ensure that security requirements for every third party that could affect the cloud service are put in place, according to the potential level of impact in the confidentiality, integrity and availability of the cloud service.

PM.3: The CSP must define, implement and maintain a procedure to identify third parties, to evaluate the impact / risk in the cloud service, and to supervise / monitor the implementation of the security requirements by the third parties.

PM.4: The CSPs must ensure that third parties also apply security controls to meet the applicable security requirements in their providers (fourth parties).

PM.5: The CSPs must define and implement a notification mechanism to ensure that information security incidents at their providers are considered also in their incident management procedure.

3.10 Incident Management

3.10.1 High level security objective

The CSP must define and implement an approach that manages information security incidents. This approach should include, among other aspects, procedures, roles, responsibilities, communication mechanisms through the appropriate channels to the relevant stakeholders in a timely manner, evidence collection mechanisms and classification, and lessons learned. All these shall be done in accordance to the regulation in force.

3.10.2 Detailed security objectives

IM.1: The CSP must define and implement the responsibilities for incident management.

IM.2: The CSP must define, document, implement, monitor and communicate a procedure to be able to respond to that information security incidents in a fast, efficient and orderly manner. This procedure should include, among other aspects, incident planning and preparation, monitoring and logging of that information security incidents, handling of that information security incidents, and response management (e.g. escalation).

IM.3: The CSP must report information security events to the established stakeholders (e.g. CERTS) through the appropriate management channels as quickly as possible and in agreement with the documented procedures and according to the regulation in place.

IM.4.: The CSP must define, document and implement the mechanisms to classify information security incidents and assess if an incident is to be qualified as an information security one, following what the regulation states.

IM.5: The employees and contractors using the organization's information systems and services of a CSP must be required to note and report any observed or suspected information security weaknesses in services or systems.

IM.6: The CSP must define, document, implement and maintain a procedure for the collection, acquisition and preservation of information related to the information security incidents, which can serve as evidence.

IM.7: The CSP must collect, preserve and keep in an internal public repository the knowledge gained from analysing and resolving information security incidents, with the aim of reducing the likelihood or impact of future that information security incidents.

3.11 Business Continuity and disaster recovery

3.11.1 High level security objective

The CSP must define, implement and maintain plans for business continuity and disaster recover to ensure that the cloud service is always available but with the highest integrity.

3.11.2 Detailed security objectives

BC.1: The CSP must define, document and communicate all information security requirements, potential problematic situations (e.g. malfunctions), threats, metrics and their acceptable thresholds

for those services not working properly (e.g. recovery time objective, mean time between failures, mean time to recover).

BC.2: the CSP must define, document, implement and monitor a business continuity plan, including contingency plans and recovery activities. This plan shall include issues such as the information security controls within business continuity and recovery processes, compensation controls, steps on how to restore a cloud service, as well as a prioritized list of services to restore, roles and responsibilities, in order to ensure that the required degree of continuity of the cloud service is ensured at all times.

BC.3: The CSP must ensure the validity and effectiveness of its business continuity and recovery plans by executing drills and tests at regular intervals. The results of such drills and tests must be documented, and the plans updated accordingly.

BC.4: The CSP must ensure the availability of its services through the implementation of redundancy mechanisms (e.g. in components, in the architecture, …). The risks related to redundancy that can cause integrity and confidentiality issues must be considered.

3.12 Compliance

3.12.1 High level security objective

The CSP must ensure and provide the means to assure compliance with the applicable regulations, legislation as well as contractual and business requirements.

3.12.2 Detailed security objectives

C.1: The CSP must achieve a clear understanding of the applicable legal and contractual security requirements that it needs to comply with.

C.2: The CSP must safeguard the conformity with legal requirements such as Intellectual Property Rights, use of cryptographic controls and privacy requirements.

C.3: The CSP must ensure that its contract is aligned with legal and business requirements.

C.4: The CSP must ensure that its records are protected from destruction, forgery, non-authorized access or publications in agreement with the legislative, regulatory, contractual and business requirements in place.

C.5: The CSP must ensure that information security is managed and operated in agreement with the policies and procedures defined in the organization.

3.13 Security Assessment

3.13.1 High level security objective

The CSP must establish and maintain procedures to review the information security at planned intervals or when significant changes occur, and results are reported to the appropriate management levels and clients (where suitable). The review is conducted by qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider.

3.13.2 Detailed security objectives

SA.1: The CSP must define, document, implement, monitor and maintain procedures to test the network and the information systems underpinning the cloud services.

SA.2: The top management of a CSP must be notified of regular compliance reviews.

SA.3: The CSP must conduct internal audits as well as independent reviews performed of IT systems and processes, including virtualized environments, networks and so on, to ensure the compliance with the organization's policies and standards (including technical compliance examination).

3.14 Interoperability and Portability[6]

3.14.1 High level security objective

The CSP must use standards and implement practices which allow customers to interface with other cloud services. The Cloud provider should also implement practices that enable customers, if needed, to recover their data and migrate to other providers offering similar services.

3.14.2 Detailed security objectives

IP.1: The CSP must make available Information about APIs and formats to support interoperability and porting.

IP.2: The CSP must make available mechanisms for customers to be able to retrieve their data in a machine-readable format at the end of the contract.

IP.3: The CSP must define and implement procedures to facilitate the data transfer. These should also be agreed with the customer of the cloud service.

IP.4: The CSP must make available measures to protect the porting of customer data and applications. This includes the use network controls to protect the information and the integrity of the network.

3.15 System Security and Integrity

This section aims at the definition of security objectives that ensure that best practices to achieve and maintain an adequate security level of software and systems and that these are systematically applied during development and deployment by the cloud service provider. The scope includes both software development conducted by the cloud service provider itself and the use and deployment of third-party components including open source as well as – most common in practice – any blend of concepts in-between those.

In essence, the requirements defined here require the cloud provider to establish a secure development lifecycle, i.e. a set of principles and processes that ensure that security is considered to be an integral element during design and development and not brought in after-the-fact.

The objectives acknowledge the agility and speed of cloud development, deployment and operation ("DevOps"), the distributed nature of the software supply chain including open source libraries, as well

[6] The objectives presented here are to be complementary to the Code of Conducts defined for IaaS and SaaS in the SWItching and POrtability self-regulatory group (SWIPO). Please refer to the Code of Conduct defined for IaaS and SaaS for more information.

as the varying nature of security contexts, e.g., the same microservice possibly used in different applications.

This section further acknowledges the need for integrating security into the lifecycle of a product or a service, leading to a focus on the processes applied during their lifecycle. In addition, this focus on the secure development and deployment life cycle facilitates the scalability of the approach by allowing to evaluate the processes themselves and their enforcement in a development project rather than the evaluation of the individual product characteristics. By doing so, for instance, a regular update of a software service can be evaluated (and certified) faster if the same processes have been applied. In turn, this leads to requirements on security functions of systems not being stated in this section but in related other sections of this document.

3.15.1 High level security objective

The CSP must manage, define, implement, and monitor the processes needed for the design, development and deployment[7] of all used software artefacts, software systems as well as their connectivity, necessary to provide the cloud service. Such processes shall cover the complete system lifecycle, from design to operation, including updates and patches, and both internal (from the CSP itself) and external (from outsourced parties, including third party components and open source software) developments.

3.15.2 Detailed security objectives

SSI.1: The CSP must define, document, execute and control processes that ensure the security of software artefacts and software systems as well as their connectivity used to implement the cloud service. This includes:

- Process controls to ensure the correct and effective implementation of technical security measures (security functions) required in other sections of this document,

[7] Example process elements for a secure development lifecycle as required by the detailed control objective include, for example:

- system/product/service description including the relevant security context and environment
- threat model and risk assessment following an established threat modelling approach
- statement of security objectives based on the threat and risk analysis
- statement of security functionality
- mapping between security objectives and security functionality
- state-of-the-art security analysis and testing of code (SAST, DAST, penetration testing), i.e., use of best-in-class tools and techniques and their combination
- security analysis of 3rd party components including open source, use of certified components
- secure deployment, integrity protection of software artefacts
- security response processes and patch processes

3rd party components also include applications of software providers that are deployed on a platform or infrastructure cloud offering. The cloud provider is required to perform a security analysis/risk assessment as part of a vetting/on boarding process for such deployments. The security analysis focuses on both legal compliance and also on the potential impact of the application's security characteristics (or lack thereof) on the infrastructure, platform or other tenants, respectively.

Regarding their own development efforts, organisations that are compliant with ISO 27034 are expected to meet many of the requirements of this section, having installed an Organization Normative Framework, providing an Organization ASC (Application Security Control) Library and having established process elements covering the assessment of the application security risk and the selection of ASCs to achieve a desired Level of Trust.

- The establishment of a secure development lifecycle for the cloud provider's own software and system developments.

For own developments of the cloud service provider, the secure development lifecycle should include controls that:

1. allow the assessment of the security risk associated with each development effort,
2. facilitate the instantiation of the lifecycle process controls following the risk assessment and providing adequate security,
3. produce evidence for the control selection and the application of each selected control during the development effort,
4. include secure delivery and deployment processes maintaining system integrity
5. cover secure system update and patching, ensuring the timely application of security patches to fix known vulnerabilities,
6. include a security response process that manages the identification, reporting and fixing of vulnerabilities,
7. each control of the secure development lifecycle is required to include validation elements that produce and check evidence for their application. The application and execution of the controls is regularly checked based on the documents and artefacts produced by the processes.

For the usage of 3rd party components and technical services, including open source software contributions, the secure development lifecycle should include controls that:

1. define a vetting or on boarding process for 3rd party components, including security requirements following a risk assessment of the component and its environment,
2. include secure delivery and deployment processes maintaining system integrity,
3. include automated process for regular analysis of vulnerabilities of 3rd party components as well as the mitigation of such vulnerabilities,
4. each control of the secure development lifecycle is required to include validation elements that produce and check evidence for their application. The application and execution of the controls is regularly checked based on the documents and artefacts produced by the processes.

3.16 Change & Configuration Management

3.16.1 High level security objective

The CSP must define, document, implement, manage and monitor a process that controls the changes to the organization, business and development processes, software assets and information processing that can affect the information security.

3.16.2 Detailed security objectives

CCM.1: The CSP must define, implement and monitor a change and configuration management process that safeguards the changes performed to all information systems required for the development, deployment and operation of a cloud service.

CCM.2: the CSP must define, implement and maintain a classification and a prioritization scale of changes.

CCM.3: The CSP must define, implement and maintain a strategy to test the performed changes in the integration (development) environment, before they are promoted to the production one.

CCM.4: The CSP must define, implement and maintain a risk assessment procedure that allows to analyse the impact of such change.

CCM.5: The CSP must implement mechanisms to record the performed changes, including reasons for the change, date, responsible, among other aspects, so as to ease the auditing procedures.

CCM.6: The CSP must define, implement and maintain a procedure to return to the situation previous to the performed change.

CCM.7: The CSP must define and implement a change approval process.

CCM.8: The CSP must define and implement a process to communicate all changes to the relevant stakeholders.

3.17 Risk Management

3.17.1 High level security objective

The CSP must define, establish, implement and maintain a governance and risk management process, covering the entire lifecycle of the provision of a cloud service.

3.17.2 Detailed security objectives

RM.1: The CSP must define, document and implement a risk management policy that covers the entire cloud service provision (including, where technically feasible, the whole cloud supply chain and underlying IaaS/PaaS/SaaS), as well as the whole cloud service life cycle.

RM.2: The CSP must periodically carry out its risk assessment by using a documented method that guarantees reproducibility and comparability of the approach.

RM.3: The CSP provider must take into account in the risk assessment:

- the cloud service customer's data classification/criticality;
- the current security posture provided by the implemented technical and organizational controls.
- Contextual information related to the cloud service, which may have effects on its attack surface (e.g., internet connectivity)

RM.4: The CSP must also consider other sources of risks such as the ones derived from assessing threats to the organization associated with PII. For this purpose, it is recommended taking into account the organization's overall business strategy and objectives.

RM.5: When there are specific legal, regulatory or sector-specific requirements linked to the type of information entrusted by the cloud service customer to the cloud service provider, the latter must consider them for its risk assessment.

RM.6: The CSP must categorized the identified risks according to their criticality, and treated accordingly (e.g., by mitigating the risk through the implementation of the corresponding security controls, by transferring the risks, or by accepting the risk)

RM7: The risk owner of the CSP must formally accept the residual risks identified in the risk assessment, which were not feasible to mitigate in the risk treatment stage. However, it is not valid the acceptance of risks associated to requirements defined in this document and which were not implemented by the cloud service provider.

RM8: The CSP must update the risk assessment either given a defined frequency, or whenever there are significant changes affecting the security posture of the cloud service.

Annex 1a - High level Gap Analysis

This annex presents the current version of the high-level gap analysis.

Table 4. High level Gap Analysis

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Information Security Policies	CCSM-ENISA SO 01 - Information security policy CCSM-ENISA SO 03 - Security roles	C5 OIS-01 Information security management system (ISMS) C5 SA-01 Documentation, communication and provision of policies and instructions C5 SA-02 Review and approval of policies and instructions C5 SA-03 Deviations from existing policies and instructions C5 OIS-03 Authorities and responsibilities s in the framework of information security C5 OIS-04 Separation of functions C5 OIS-05 Contact with relevant government agencies and interest groups	SecNum 5.1. Principles SecNum 5.2. Information security policy SecNum 6.1. Functions and responsibilities linked to information security SecNum 6.2. Segregation of tasks SecNum 6.3. Relations with the authorities SecNum 6.4. Relations with specialised work groups SecNum 6.5. Information security in project management HYG33: Adopt security policies dedicated to mobile devices	ISO 27002: 5.1.1 A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties. ISO 27002: 5.1.2 The policies for information security should be review at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. ISO 27002: 6.1.1 All information security responsibilities should	ISO 27017: CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	ISO 27018: 5.1.1 A statement to achieving compliance with applicable PII protection legislation and the contractual terms. ISO 27018: 6.1.1 The public cloud PII processor should designate a point of contact regarding the processing of PII under the contract. ISO 27018 A.9.2 Retention period for administrative

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		C5 OIS-06 Policy for the organization of the risk management C5 OIS-02 Strategic targets regarding information security and responsibility of the top management C5 OIS-07 Identification, analysis, assessment and handling of risks		be defined and allocated. ISO 27002: 6.1.2 Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets ISO 27002: 6.1.3 Appropriate contacts with relevant authorities should be maintained. ISO 27002: 6.1.4 Appropriate contacts with special interest groups or other specialist security forums and		security policies and guidelines

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				professional associations should be maintained. ISO 27002: 6.1.5 Information security should be addressed in project management, regardless of the type of the project. ISO 27002: 6.2.1 A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices. ISO 27002: 6.2.2 A policy and supporting security measures should be implemented to protect information accessed, processed or		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				stored at teleworking sites.		
Personnel & Training	CCSM-ENISA SO 05 - Background checks CCSM-ENISA SO 06 - Security knowledge and training CCSM-ENISA SO 07 - Personnel changes	C5 HR-01 Security check of the background information C5 HR-02 Employment agreements C5 HR-03 Security training and awareness- raising programme C5 HR-04 Disciplinary measures C5 HR-05 Termination of the employment relationship or changes to the responsibilities	SecNum 7.1. Selection of candidates SecNum 7.2. Conditions for hire SecNum 7.3. Awareness, learning and training on information security SecNum 7.4. Disciplinary process SecNum 7.5. Rupture, term or modification in the labour contract HYG1 Train the operational Team in Information System Security (which include not only technical but organizational and regulatory training) HYG2 Raise user awareness about basic	ISO 27002: 7.1.1 Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. ISO 27002: 7.1.2 The contractual agreements with employees and contractors should		ISO 27018: 7.2.2 Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor. ISO 27018: A.10.1 Confidentiality or non-disclosure agreements

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			information security (this target the end user on a system, here it shall be interpreted as an user of the Cloud Service offered) HYG24 Protect your professional email (beside technical protection, this rules emphasis on user awareness for the use of his email, which is more a matter of training) HYG39 Designate a point of contact in information system security and make sure staff are aware of him or her	state their and the organization's responsibilities for information security. ISO 27002: 7.2.1 Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. ISO 27002: 7.2.2 All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				and procedures, as relevant for their job function. ISO 27002: 7.2.3 There should be a formal and communicated disciplinary process in place to take action against employees who have committed and information security breach. ISO 27002: 7.3.1 Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				contractor and enforced.		
Asset Management	CCSM-ENISA SO 14 - Asset management	C5 AM-01 Asset inventory C5 AM-02 Assignment of persons responsible for assets C5 AM-03 Instruction manuals for assets C5 AM-04 Handing in and returning assets C5 AM-05 Classification of information C5 AM-06 Labelling of information and handling of assets C5 AM-07 Management of data media C5 AM-08 Transfer and removal of assets	SecNum 8.1. Inventory and property of assets SecNum 8.2. Restitution of assets SecNum 8.3. Identification of the information security needs SecNum 8.4. Marking and manipulating information SecNum 8.5. Management of removable media HYG4: Identify the most sensitive assets and maintain a network diagram (this diagram is a simple one, helping to locate where sensitive assets are localized)	ISO 27002: 8.1.1 Information, other assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. ISO 27002: 8.1.2 Assets maintained in the inventory should be owned. ISO 27002: 8.1.3 Rules for the acceptable use of information and of assets associated with information and information processing facilities	ISO 27017: CLD.8.1.5 Removal of cloud service customer assets	ISO 27018: 8; Reference to ISO 27002, Section 8 ISO 27018: Annex 9.3: PII return, transfer and disposal

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				should be identified, documented and implemented. ISO 27002: 8.1.4 All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. ISO 27002: 8.2.1 Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. ISO 27002: 8.2.2 An appropriate set of		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization. ISO 27002: 8.2.3 Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization. ISO 27002: 8.3.1 Procedures should be implemented for the management of removable media in		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				accordance with the classification scheme adopted by the organization. ISO 27002: 8.3.2 Media should be disposed of securely when no longer required, using formal procedures. ISO 27002: 8.3.3 Media containing information should be protected against unauthorized access, misuse or corruption during transportation.		
Identity & Access Management	CCSM-ENISA SO 10 - Access control to network and information systems	C5 IDM-01 Policy for system and data access authorisations C5 IDM-02 User registration C5 IDM-03 Granting and change	SecNum 9.1. Policies and access control SecNum 9.2. Registering and deregistering users SecNum 9.3. Management of access rights	ISO 27002: 9.1.1 An access control policy should be established, documented and reviewed based on business and information security	ISO 27017: CLD.9.5.1 Segregation in virtual computing environments ISO 27017: CLD.9.5.2 Virtual	ISO 27018: 9.2 Public cloud PII processor should enable the cloud service customer to manage access by cloud service

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		(provisioning) of data access authorisations C5 IDM-09 Handling of emergency users C5 IDM-07 Non-disclosure of authentication information C5 IDM-06 Administrator authorisations C5 IDM-05 Regular review of data access authorisations C5 IDM-04 Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship C5 IDM-08 Secure login methods C5 IDM-10 System-	SecNum 9.4. Review of user access rights SecNum 9.5. Management of user authentications SecNum 9.6. Access to administration interfaces SecNum 9.7. Restriction of access to information HYG5: have an exhaustive inventory of privileged account and keep it updated (not only administrator but include user with extended privileges) HYG8: Identify each individual accessing the system by name and distinguish the user/administrator role (this control applies to both end user and	requirements. ISO 27002: 9.1.2 Users should only be provided with access to the network and network services that they have been specifically authorized to use. ISO 27002: 9.2.1 A formal registration and de-registration process should be implemented to enable assignment of access rights. ISO 27002: 9.2.2 A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	Machine Hardening	users under the cloud service customer's control ISO 2018: 9.2.1 Procedures for user registration and de-registration should address the situation where user access control is compromised ISO 2018: 9.4.2 Public cloud PII processor should provide secure log-on procedures ISO 27018:Annex A.10.8 Unique Use of User IDs

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		side access control C5 IDM-11 Password requirements and validation parameters C5 IDM-12 Restriction and control of administrative software C5 IDM-13 Control of access to source code	personnel. It shall be further refined between these two categories) HYG9: Allows the appropriate rights to the information system's sensitive resources. HYG29: Reduce administration rights on workstations to strictly operational needs	ISO 27002: 9.2.3 The allocation and use of privileged access rights should be restricted and controlled. ISO 27002: 9.2.4 The allocation of secret authentication information should be controlled through a formal management process. ISO 27002: 9.2.5 Asset owners should review users' access rights at regular intervals. ISO 27002: 9.2.6 The access rights of all employees and external party users to information and information processing facilitating		ISO 27018: Annex A.10.9 Records of Authorized Users ISO 27018: Annex A.10.10 User ID Management ISO 27018: A.10.13 Access to data on pre-used data storage space

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				should be removed upon termination of their employment, contract or agreement, or adjusted upon change. ISO 27002: 9.3.1 Users should be required to follow the organization's practices in the use of secret authentication information. ISO 27002: 9.4.1 Access to information and application system functions should be restricted in accordance with the access control policy. ISO 27002: 9.4.2 Where required by the access control policy, access to systems and		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				applications should be controlled by a secure log-on procedure. ISO 27002: 9.4.3 Password management systems should be interactive and should ensure quality passwords. ISO 27002: 9.4.4 The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. ISO 27002: 9.4.5 Access to program source code should be restricted.		
Cryptography & Key management		C5 KRY-01 Policy for the use of encryption procedures and key	SecNum 10.1. Encryption of the data stored	ISO 27002: 10.1.1 A policy on the use of cryptographic controls		ISO 27018: 10 Reference to ISO 27002; Sections

EC-CLOUD CATEGORY	CCSM-ENISA [1]	C5 GERMANY [4]	SecNum FRANCE [3]	ISO 27002 [12]	ISO 27017 (Only deltas included) [6]	ISO 27018 (Reference plus deltas included) [7]
		management C5 KRY-02 Encryption of data for transmission (transport encryption) C5 KRY-03 Encryption of sensitive data for storage C5 KRY-04 Secure key management	SecNum 10.2. Flow encryption SecNum 10.3. Password hashing SecNum 10.4. Non-repudiation SecNum 10.5. Management of secrets HYG10: Set and verify the rules for the choice and size of password (determines in fine the real strength of cryptography key used for encryption) HYG13: prefer a two-factor authentication when possible HYG31: Encrypt sensitive data, in particular on hardware that can potentially be lost	for protection of information should be developed and implemented. ISO 27002: 10.1.2 A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.		10.1.1, 10.1.2 ISO 27018 Annex A 10.6.: Encryption of PII transmitted over public data-transmission networks

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Physical Infrastructure Security	CCSM-ENISA SO 08 - Physical and environmental security	C5 PS-01 Perimeter protection C5 PS-02 Physical site access control C5 PS-03 Protection against threats from outside and from the environment C5 PS-04 Protection against interruptions caused by power failures and other such risks C5 PS-05 Maintenance of infrastructure and devices	SecNum 11.1.1. Physical security perimeters: Public areas SecNum 11.1.2. Physical security perimeters: Private areas SecNum 11.1.3. Physical security perimeters: Sensitive areas SecNum 11.2.1. Physical access control: Private areas SecNum 11.2.2. Physical access control: Sensitive areas SecNum 11.3. Protection against outside and environmental threats SecNum 11.4. Working in private and sensitive areas SecNum 11.5. Delivery and loading areas	ISO 27002: 11.1.1 Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. ISO 27002: 11.1.2 Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. ISO 27002: 11.1.3 Physical security for officers, rooms and facilities should be designed and applied. ISO 27002: 11.1.4 Physical protection		ISO 27018: 11; reference to ISO 27002; Sections 11.1, 11.2 ISO 27018: A.10.7 Secure disposal of hardcopy materials

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			SecNum 11.6. Wiring security SecNum 11.7. Hardware maintenance SecNum 11.8. Disposal of assets SecNum 11.9. Secured recycling of hardware SecNum 11.10. Hardware on hold for use HYG26: Control and protect the access to the server rooms and technical areas	against disasters, malicious attack or accidents should be designed and applied. ISO 27002: 11.1.5 Procedures for working in secure areas should be designed and applied. ISO 27002: 11.1.6 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. ISO 27002: 11.2.1 Equipment should be		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. ISO 27002: 11.2.2 Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. ISO 27002: 11.2.3 Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. ISO 27002: 11.2.4		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				Equipment should be correctly maintained to ensure its continued availability and integrity. ISO 27002: 11.2.5 Equipment, information or software should not be taken off-site without prior authorization. ISO 27002: 11.2.6 Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises. ISO 27002: 11.2.7 All items of equipment containing storage		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. ISO 27002: 11.2.8 Users should ensure that unattended equipment has appropriate protection. ISO 27002: 11.2.9 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Operational Security	CCSM-ENISA SO 12 - Operating procedures	C5 RB-02 Capacity management – monitoring C5 RB-04 Capacity management – control of resources C5 RB-05 Protection against malware C5 RB-08 Data backup and restoration - regular tests C5 RB-13 Logging and monitoring - storage of the logs C5 RB-15 Logging and monitoring - configuration C5 RB-21 Handling of vulnerabilities, malfunctions and errors - check of open vulnerabilities C5 RB-01 Capacity	SecNum 12.1. Documented operating procedures SecNum 12.2. Managing change SecNum 12.3. Segregation of the development, test and operating environments SecNum 12.4. Measures against malicious code SecNum 12.5. Information backup SecNum 12.6. Logging of events SecNum 12.7 Protection for logged information SecNum 12.8 Clock synchronization SecNum 12.9. Analysis and correlation of events SecNum 12.11. Technical vulnerability	ISO 27002: 12.1.1 Operating procedures should be documented and made available to all users who need them. ISO 27002: 12.1.2 Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. ISO 27002: 12.1.3 The use of resources should be monitored, turned and projections made of future capacity requirements to ensure the required system performance.	ISO 27017: CLD.12.1.5 Administrator's operational security ISO 27017: CLD.12.4.5 Monitoring of Cloud Services	ISO 27018: 12, reference to ISO 27002 Section 12 ISO 27018: 12.4.1 Cloud PII processor should define procedures regarding if, when and how log information can be made available to or usable by customer ISO 27018: 12.4.2 Log information recorded may contain PII. Measures should be put in place to ensure only use for its intended purposes

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		management – planning C5 RB-03 Capacity management – data location C5 RB-06 Data backup and restoration - concept C5 RB-07 Data backup and restoration - monitoring C5 RB-09 Data backup and restoration - storage C5 RB-10 Logging and monitoring - concept C5 RB-11 Logging and monitoring - meta data C5 RB-12 Logging and monitoring - critical assets C5 RB-14 Logging and	management SecNum 12.12. Administration. HYG6: Organize the procedure relating to user joining, departing and changing positions (include personnel, but can be interpreted to customer subscribing any offers for joining and departing) HYG11: protect password on stored system (avoid post-it, and use electronic safe solution instead. Protection of password should be part of the operational procedures) HYG16: use a centralized management tool to standardize security	ISO 27002: 12.1.4 Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. ISO 27002: 12.2.1 Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. ISO 27002: 12.3.1 Backup copies of information, software and system images should be taken and		ISO 27018: A.10.2 Restriction of the creation of hardcopy material ISO 27108: A.10.3 Control and logging of data restoration

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		monitoring - accountability C5 RB-16 Logging and monitoring - availability of the monitoring software C5 RB-17 Handling of vulnerabilities, malfunctions and errors - concept C5 RB-18 Handling of vulnerabilities, malfunctions and errors - penetration tests C5 RB-19 Handling of vulnerabilities, malfunctions and errors - integration with change and incident management C5 RB-20 Handling of vulnerabilities, malfunctions and	policies (backing security operation by a standardized and automated tool)	tested regularly in accordance with an agreed backup policy. ISO 27002: 12.4.1 Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. ISO 27002: 12.4.2 Logging facilities and log information should be protected against tampering and unauthorized access. ISO 27002: 12.4.3 System administrator and system operator activities should be logged and the logs protected and regularly reviewed.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		errors - involvement of the cloud customer C5 RB-22 Handling of vulnerabilities, malfunctions and errors - system hardening C5 RB-23 Segregation of stored and processed data of the cloud customers in jointly used resources		ISO 27002: 12.4.4 The clocks of all relevant information processing systems within and organization or security domain should be synchronised to a single reference time source. ISO 27002: 12.5.1 Procedures should be implemented to control the installation of software on operational systems. ISO 27002: 12.6.1 Information about technical vulnerabilities of information systems being used should be obtained in a timely		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. ISO 27002: 12.6.2 Rules governing the installation of software by users should be established and implemented. ISO 27002: 12.7.1 Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Communications Security		C5 KOS-03 Cross-network access C5 KOS-02 Monitoring of connections C5 KOS-04 Networks for administration C5 KOS-05 Segregation of data traffic in jointly used network environments C5 KOS-08 Confidentiality agreement C5 KOS-07 Policies for data transmission C5 KOS-01 Technical safeguards C5 KOS-06 Documentation of the network topology	SecNum 10.2. Flow encryption SecNum 13.1. Map of the information system. SecNum 13.2. Network partitioning SecNum 13.3. Network monitoring HYG18: Encrypt sensitive data sent through the internet (apply to end user connection, data link for replication/redundancy, remote administration link etc..) HYG19: Segment the network and implement a partitioning between these areas HYG20: ensure the security of WiFi access network and that uses are separated	ISO 27002: 13.1.1 Networks should be managed and controlled to protect information in systems and applications. ISO 27002: 13.1.2 Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. ISO 27002: 13.1.3 Groups of information services, users and information systems should be segregated	ISO 27017: CLD.13.1.4 Alignment if security management for virtual and physical networks	ISO 27018: 13; Reference to ISO 27002 Section 13 ISO 27018 Annex A 10.6.: Encryption of PII transmitted over public data-transmission networks

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			HYG21: use secure network protocol when they exists HYG22: implements a secure gateway to the internet (this implies all access to Internet are known and secured) HYG23: Segregate the services visible from the Internet from the rest of the Information System HYG25: Secure the dedicated network interconnections with partners HYG28: use a dedicated and separated network for information system administration HYG32: Secure the network connection of devices used in a mobile working situation	on networks. ISO 27002: 13.2.1 Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. ISO 27002: 13.2.2 Agreements should address the secure transfer of business information between the organization and external parties. ISO 27002: 13.2.3 Information involved in electronic messaging should be appropriately protected.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				ISO 27002: 13.2.4 Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.		
Procurement Management (Supply change management)	CCSM-ENISA SO 04 - Security in Supplier relationships CCSM-ENISA SO 09 - Security of supporting utilities	C5 BEI-01 Policies for the development / procurement of information systems C5 BEI-03 Policies for changes to information systems C5 BEI-09 Review of proper testing and approval C5 BEI-11 System landscape C5 BEI-02	SecNum 14. Acquisition, development and maintenance of information systems SecNum 14.1. Secure development policy SecNum 14.2. Procedures for controlling changes to the system SecNum 14.3. Technical review of the applications after a	ISO 27002: 14.1.1 The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems. ISO 27002: 14.1.2 Information involved in application services		ISO 27018: 14; reference to ISO 27002 Section 14 ISO 27018: 15; reference to ISO 27002 Section 15 ISO 27018: Annex A7.1: Disclosure of Sub-Contracted PII Processing ISO 27018:

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		Outsourcing of the development C5 DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider C5 DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider C5 BEI-12 Separation of functions	change made to the operating platform SecNum 14.4. Secure development environment SecNum 14.5. Outsourced development SecNum 14.6. System security and compliance test SecNum 14.7. Protection of test data SecNum 15. Relations with third parties SecNum 15.1. Identification of third parties SecNum 15.2. Security in the agreements made with third parties SecNum 15.3. Monitoring and review of third party services	passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. ISO 27002: 14.1.3 Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. ISO 27002: 14.2.1 Rules for the development of		A.10.11 Data processing contract measures ISO 27018: Annex A 10.12 Sub-contracted PII processing

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			SecNum 15.4. Managing changes made in the services of third parties SecNum 15.5. Confidentiality undertakings HYG3 Control Outsourced Service (studying offer, impose some requirements like contract reversibility, prefer standard and open format to proprietary solutions) HYG42 Favours the use of products and services qualified by ANSSI. This could be translated as « favour products and service that have been formally certified under the European Cyber Certification Scheme »	software and systems should be established and applied to developments within the organization. ISO 27002: 14.2.6 Organizations should establish and appropriately protect secure developments environments for system development and integration efforts that cover the entire system development lifecycle. ISO 27002: 14.2.7 The organization should supervise and monitor the activity of outsourced system development. ISO 27002: 14.2.8 Testing of security		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				functionality should be carried out during development. ISO 27002: 14.2.9 Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. ISO 27002: 14.3.1 Test data should be selected carefully, protected and controlled. ISO 27002: 15.1.1 Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				the supplier and documented. ISO 27002: 15.1.2 All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. ISO 27002: 15.1.3 Agreements with suppliers should include requirements to address the information security risks associated with information and communications		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				technology services and product supply chain. ISO 27002: 15.2.1 Organizations should regularly monitor, review and audit supplier service delivery. ISO 27002: 15.2.2 Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				involved and re-assessment of risks.		
Incident Management	CCSM-ENISA SO 15 – Security incident detection and response CCSM-ENISA SO 16 – Security incident reporting	C5 SIM-01 Responsibilities and procedural model C5 SIM-03 Processing of security incidents C5 SIM-04 Documentation and reporting of security incidents C5 SIM-05 Security incident event management C5 SIM-07 Evaluation and learning process C5 SIM-02 Classification of customer systems C5 SIM-06 Duty of the users to report security incident to a central body	SecNum 16. Managing incidents linked to information security SecNum 16.1. Responsibilities and procedures SecNum 16.2. Reporting linked to information security SecNum 16.3. Assessment of events linked to information security and decision making SecNum 16.4. Response to incidents linked to information security SecNum 16.5. Learning from incidents linked to information security SecNum 16.6. Collecting proof	ISO 27002: 16.1.1 Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. ISO 27002: 16.1.2 Information security events should be reported through appropriate management channels as quickly as possible. ISO 27002: 16.1.3 Employees and contractors using the organization's information systems and services should be		ISO 27018: 16, Reference to ISO 27002, Section 16 ISO 27018: Annex A.9.1 Notification of a data breach involving PII

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			HYG40 Define a security incident management procedure	required to note and report any observed or suspected information security weaknesses in systems or services. ISO 27002: 16.1.4 Information security events should be assessed and it should be decided if they are to be classified as information security incidents. ISO 27002: 16.1.5 Information security incidents should be responded to in accordance with the documented procedures. ISO 27002: 16.1.6 Knowledge gained from analysing and resolving information		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				security incidents should be used to reduce the likelihood or impact of future incidents. ISO 27002: 16.1.7 The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		
Business Continuity	CCSM-ENISA SO 17 –Business continuity CCSM-ENISA SO 18 - Disaster recovery capabilities	C5 BCM-01 Top management responsibility C5 BCM-02 Business impact analysis policies and procedures C5 BCM-04 Verification, updating and testing of the	SecNum 17. Continuity of activity SecNum 17.1. Organization of the continuity of activity SecNum 17.2. Implementing continuity of activity SecNum 17.3. Check, review and evaluate the	ISO 27002: 17.1.1 The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or		ISO 27018:12.3.1 Information backup ISO 27018: 17 Reference to ISO 27002, Section 17

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		business continuity C5 BCM-03 Planning business continuity C5 BCM-05 Supply of the computing centres	continuity of activity SecNum 17.4. Availability of the means for information processing HYG37: Define and apply a backup policy for critical components (applicable equally for disaster recovery) There is no explicit requirement toward disaster recovery in SecNumCloud. However, some requirements are close to a disaster recovery, thus they're referenced here. SecNum 12.5. Information backup SecNum 11.3. Protection against outside and	disaster. ISO 27002: 17.1.2 The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during and adverse situation. ISO 27002: 17.1.3 The organization should verify the established information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. ISO 27002: 17.2.1		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			environmental threats (more preventing than recovering) HYG37: Define and apply a backup policy for critical components (applicable equally for business continuity) SecNum 19.1 Service Agreement h) (service availability)	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.		
Compliance	CCSM-ENISA SO 22 – Checking compliance CCSM-ENISA SO 27 - Cloud monitoring and log access CCSM-ENISA SO 19 - Monitoring and logging policies	C5 COM-01 Identification of applicable legal, contractual and data protection requirements C5 COM-02 Planning independent, external audits C5 COM-03 Carrying out independent, external audits	SecNum 5.3 Risk assessment. Clause 4 SecNum 18.1 Identification of the legislation and the contractual requirements that apply SecNum 18.2 Independent review of information security SecNum 18.3 Compliance with security policies and	ISO 27002: 18.1.1 All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system		ISO 27018: 18; Reference to ISO 27002, Section 18 with an extension in 18.2.1: Independent reviews serving as compliance instrument for the cloud customer

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			standards SecNum 18.4 Technical compliance examination SecNum 19.1 Service agreement SecNum 19.2 Location of data SecNum 19.3 Regionalization SecNum 19.4 End of contract	and the organization. ISO 27002: 18.1.2 Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. ISO 27002: 18.1.3 Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory,		ISO 27018: Annex A 11.1: Disclosure of geographical location of PII ISO 27018: Annex A 11.2 Intended destination of PII

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				contractual and business requirements. ISO 27002: 18.1.4 Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. ISO 27002: 18.1.5 Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations. ISO 27002: 18.2.1 The organization's approach to managing information security and its		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. ISO 27002: 18.2.2 Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				ISO 27002: 18.2.3 Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.		
Security Assessment	CCSM-ENISA SO 21 - Security assessments CCSM-ENISA SO 20 - System tests	C5 SPN-01 Notification of the top management C5 SPN-02 Internal audits of the compliance of IT processes with internal security policies and standards C5 SPN-03 Internal audits of the compliance of IT systems with internal security policies and standards	SecNum 18.2 Independent review of information security HYG38: Undertake regular controls and security audits then apply the associated corrective actions HYG41: (for strengthening HYG38) Carry out a formal risk assessment			ISO 27018: 18.2.2; 18.2.3; Reference to ISO 27002 18.2.2; 18.2.3

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Interoperability & Portability	CCSM-ENISA SO 26 - Cloud interoperability and portability	C5 PI-01 Use of public APIs and industry standards C5 PI-02 Export of data C5 PI-03 Policy for the portability and inter- operability C5 PI-04 Secure data import and export C5 PI-05 Secure deletion of data				
System Security & Integrity	CCSM-ENISA SO 11 - Integrity of network and information systems CCSM-ENISA SO 23 - Cloud data security CCSM-ENISA SO 24 - Cloud interface security CCSM-ENISA SO 25 -		SecNum 11.8 Disposal of assets SecNum 14.7 Protection of test data HYG14: Implement a minimum of security across the whole IT stock HYG15: Protect against threat relating to the use of removable media			ISO 27018: 9.4; reference to ISO 27002 9.4

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
	Cloud software security		(include USB device, CD-ROM but our reflexion have to take into account any other way used to populate data on the cloud infrastructure in our context) HYG17: Activate and configure the firewall on workstations (this should be considered for an IAAS infrastructure, workstation won't make as much sense in a cloud infrastructure as in a regular IT system) HYG36: Activate and configure the most important component logs			

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Change & Configuration Management	CCSM-ENISA SO 13 - Change management	BEI-03 Policies for changes to information systems BEI-04 Risk assessment of changes BEI-05 Categorisation of changes BEI-06 Prioritisation of changes BEI-07 Test the changes BEI-08 Rollback of changes BEI-09 Review of proper testing and approval BEI-10 Emergency changes	SecNum 12.2 Managing change SecNum 14.2. Procedures for controlling changes to the system SecNum 14.3. Technical review of the applications after a change made to the operating platform HYG34: Define an update policy for the components of the information system HYG35: Anticipate the software and system end of life/maintenance and limit software reliance (e.g. dependency to proprietary software/solution)	14.2.2 Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures. 14.2.3 When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. 14.2.4 Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled		ISO 27018: 12.1.2; reference to ISO 27002 12.1.2

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
Risk / Threat / Vulnerability Management	CCSM-ENISA SO 02 - Risk management		SecNum 5.3 Risk assessment SecNum 12.11 Technical vulnerability management			ISO 27018: 0.3 PII protection requirements ISO 27018: 0.4 Selecting and implementing controls in a cloud computing environment
Personnel & Training	CCSM-ENISA SO 05 - Background checks CCSM-ENISA SO 06 - Security knowledge and training CCSM-ENISA SO 07 - Personnel changes	C5 HR-01 Security check of the background information C5 HR-02 Employment agreements C5 HR-03 Security training and awareness- raising programme C5 HR-04 Disciplinary measures C5 HR-05	SecNum 7.1. Selection of candidates SecNum 7.2. Conditions for hire SecNum 7.3. Awareness, learning and training on information security SecNum 7.4. Disciplinary process SecNum 7.5. Rupture, term or modification in the labour contract HYG1 Train the operational Team in	ISO 27002: 7.1.1 Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be		ISO 27018: 7.2.2 Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor. ISO 27018: A.10.1 Confidentiality or non-disclosure agreements

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
		Termination of the employment relationship or changes to the responsibilities	Information System Security (which include not only technical but organizational and regulatory training) HYG2 Raise user awareness about basic information security (this target the end user on a system, here it shall be interpreted as end user of the Cloud Service offered) HYG24 Protect your professional email (beside technical protection, this rules emphasis on user awareness for the use of his email, which is more a matter of training) HYG39 Designate a point of contact in information system	accessed and the perceived risks. ISO 27002: 7.1.2 The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security. ISO 27002: 7.2.1 Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. ISO 27002: 7.2.2 All employees of the organization and,		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
			security and make sure staff are aware of him or her	where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. ISO 27002: 7.2.3 There should be a formal and communicated disciplinary process in place to take action against employees who have committed and information security breach. ISO 27002: 7.3.1 Information security responsibilities and duties that remain		

EC-CLOUD CATEGORY	**CCSM-ENISA** [1]	**C5 GERMANY** [4]	**SecNum FRANCE** [3]	**ISO 27002** [12]	**ISO 27017 (Only deltas included)** [6]	**ISO 27018 (Reference plus deltas included)** [7]
				valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.		

Annex 2 – Milestone 2: Conformity Assessment Methodologies

1 Introduction

1.1 Purpose

The purpose of a Conformity Assessment is *to enhance the credibility* (or confidence or trust) towards stakeholders of a statement expressed by a cloud service provider (CSP) that its cloud process, product or service (including those from sub-service providers) meets the requirements of a pre-defined set of control objectives and a related set of measures, as defined under Milestone 1.

The assurance of a European certification scheme is the ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure consistency of the framework on certified ICT processes, products and services, a European cybersecurity certification scheme could specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each certificate could refer to one of the assurance levels: basic, substantial or high, while the EU statement of conformity could only refer to the assurance level basic. The assurance levels provide a corresponding degree of efforts for the evaluation of and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent cybersecurity incidents.

1.2 Methodologies

The CSPCERT WG has made an inventory of existing Conformity Assessment Methodologies that can be used as part of a Cybersecurity Certification Scheme for cloud services as defined in Point (12), Article 2 of (EC) Regulation No 765/2008 [26]: “Conformity assessment’ shall mean the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled”.

The working group took into account currently existing assessment methodologies and practices at cloud service providers in order to reduce the administrative burden on these enterprises. After due deliberation within the working group and public consultation it was decided to propose the following three Conformity Assessment Methodologies for the Certification Scheme as defined in the proposal for the EUCA [30]:

- Evidence based conformity assessment;
- Third party conformity assessment in accordance with ISO approach;
- Third party conformity assessment in accordance with International Standards on Assurance Engagements 3000/3402.

The CSPCERT WG also considered implementing some form of continuous monitoring. Based upon discussions within the working group and feedback received during the public consultation continuous monitoring is considered an important element of future certification schemes. Currently, however, continuous monitoring is not considered to be of sufficient maturity to be part of this proposal.

A detailed comparison of these three conformity assessment methodologies is provided in section 5 of this annex.

1.3 Levels of Assurance

In accordance with Article 52 of the EUCA, in the opinion of the CSPCERT working group, all three proposed conformity assessment methodologies can be used for a European cybersecurity certificate that refers to assurance level "basic". Both third-party conformity assessments can be used for a European cybersecurity certificate that refers to assurance levels "substantial" and "high".

Table 5. Conformity assessment methodologies vs. levels of assurance

Conformity assessment	**Level of Assurance**			**Result**
	Basic	Substantial	High	
Evidence based conformity assessment	X			European Cybersecurity Certificate (*)
Third party ISO based approach	X	X	X	European Cybersecurity Certificate (*)
Third party ISAE based approach	X	X	X	European Cybersecurity Certificate (*)

(*) A European cybersecurity certificate means a document issued by the relevant body attesting that a given ICT product, service or process has been evaluated for compliance with specific requirements laid down in a European cybersecurity certification scheme

1.4 Cycle approach

The conformity assessment demonstrates that the requirements have been fulfilled at a certain moment in time or over a period prior to the reporting date. The certificate has a maximum period of validity as required by Article 54(j) of the EUCA. In accordance with current common practices, the CSPCERT WG proposes a period of validity for the European Cybersecurity Certificate for cloud services of a maximum of 3 (three) years after initial issuance. This three-year certification cycle should be supported by annual surveillance evaluations by the certificate issuer. The form in which these surveillance evaluations should be performed is described in the following paragraphs.

1.5 Scope

By their nature, the services of a CSP will not be delivered by the CSP alone. A cloud service as acquired by an end user (organization) will be a collaboration of various cloud service providers under the end responsibility of, in most cases, a Software As A Service (SaaS) provider. For its service delivery this SaaS provider will use Platform As A Service (PaaS) providers, Infrastructure As A Service (IaaS) providers, Managed Service (MS) providers and in some cases other (cloud) providers. In order to complete the conformity assessment for a SaaS provider, it is relevant as a minimum, to identify the sub-service providers and assess their conformity as well. The scope of the EU Cybersecurity Certificate for Cloud Services should not be the CSP but the service (process) itself. This means that the conformity assessment should not be limited to the ultimate SaaS provider's organisation but also include relevant processes within sub-service organisations.

2 Evidence Based Conformity Assessment (EBCA)

2.1 Introduction

According to Section 79 of the EUCA it is allowed to carry out a conformity assessment under the sole responsibility of the manufacturer or provider of ICT products and services and restricted to the assurance level basic. This assessment is carried out by the provider of ICT services, products or processes, which evaluates the fulfilment of the requirements, set in a European cybersecurity certification scheme.

The CSP may issue an EU Statement of Conformity taking into account the provisions of art. 46a.

However, the CSPCERT WG, considering the fast developing (technical) world of cloud computing. is of the opinion that at least a review needs to take place by an independent party. To allow for this review the EBCA is introduced in the upcoming sections.

2.2 Assessment Approach

At the state of practice, there is no standardized method for performing an EBCA process.

A general requirement to the process can be taken Recital 88 of the EUCA: "[…] *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."*

The working group proposes an approach for EBCA similar to the one used in obtaining the Trusted Cloud label (issued by the *Kompetenznetzwerk Trusted Cloud* under patronage of the German Federal Ministry of Economic Affairs and Energy).

The CSP has to provide to the reviewer structured information about the ICT product, process or service provided and on all items of the pre-defined set of criteria of Milestone 1.

The information provided by the CSP is legally binding and should be signed off by the management of the CSP. Other documentation to be provided by the CSP include among others: copies of standard service agreements, documentation on IT security management, certificates of the service provider and its subcontractors, contacts to reference customers.

The application request is submitted to a monitoring body appointed by the National Certification Authority. This accreditation process should also make sure that all evaluation bodies are acting according to a procedures' manual describing the steps of the evaluation process and the minimum criteria for acceptance.

Subsequently, the application request is examined by the monitoring body (a qualified independent assurance provider) based on a guideline manual describing the examination process (including "must" criteria and good practices). It is the experience of the Trusted Cloud program that during the process several interviews are conducted to assert plausibility and correctness of the statements of the cloud provider. Based on this check the auditor prepares a report that is the basis for awarding the certification label.

The report is sent to the National Certification Authority for inspection and, upon successful completion, the issue of the basic certificate and the listing of the cloud service in a comprehensive directory of certified services.

As a prerequisite for this, the applicant has to sign a contract, which defines the rules of using the certification label and also the obligation to immediately notify the evaluation body or/and the National Certification Authority if any relevant changes have been made to the respective service.

Upon such notification, a re-evaluation has to be performed; if the criteria of the scheme are not met anymore the certification has to be immediately revoked/withdrawn.

2.3 Annual surveillance

The CSP has to update the documentation supporting the basic certificate on an annual basis and arrive at a conclusion regarding the continued conformity to the criteria by the product, process, service, system, person or body. The updated documentation must remain available for review by or on behalf of the National Cybersecurity Certification Authority for the remaining period of validity of the certificate. In case a significant change to the service has occurred during the cycle, a re-evaluation as described in Annex 2, 2.2 has to be performed.

2.4 Reporting and issuance of an EU basic certificate

The monitoring body will prepare a standardized report according to the standards of the National Certification Authority. The report will be kept as part of the documentation on the assessment.

This detailed report will include statements and comments of the CSP's assessor to each of the criteria of the scheme. It is important for consistency reasons and to be able to validate the final judgment whether or not to issue an EU basic certificate, to have a standard format of the procedures to be executed by the assessor and for the reports to be issued. For developing such a procedure manual and standard reporting formats use can be made of the approach described in the International Standards on Assurance Engagements. The scope of the report should comprise the service provided by the CSP and clearly identify all underlying and supporting services.

2.5 Monitoring

The National Cybersecurity Certification Authority will maintain a register of all EU basic certificate issued in its jurisdiction. This register will indicate the name of the CSP, the name of the service, the date of issuance of the EU basic certificate and the expiration date of the validity.

3 ISO based conformity assessment

3.1 Introduction

The International Standards Organization (ISO) provides a conformity assessment methodology based upon the following standards:

ISO/IEC 17000:2004 – Conformity assessment – Vocabulary and general principles [31]

ISO/IEC 17021:2015 – Conformity assessment – Requirements for bodies providing audit and certification of management systems [17]

ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services [18]

ISO 19011:2018 –Guidelines for auditing management systems [32]

ISO/IEC 17021:2015 and ISO/IEC 17065:2012 provide requirements for certification bodies regarding:

- General principles
- Legal and contractual matters
- Management of impartiality
- Liability and financing
- Organizational structure
- Resourcing
- Process
- Management system operated

ISO 19011:2018 provides detailed guidance as to the execution of the audit. The standard does not provide guidance on the assurance level to be achieved and leaves that up to the auditor's professional judgment.

3.2 Cycle approach

Both ISO/IEC 17021:2015 and ISO/IEC 17065:2012 standards show a large degree of similarity with a major difference being that ISO/IEC 17021:2015 defines a three-year audit and certification cycle whereas ISO/IEC 17065:2012 refers to the certification scheme for the validity of a certificate.

ISO/IEC 17021:2015 defines a three-year certification and audit cycle, which is executed in a phased approach:

1. Initial Certification Audit
    a. Stage 1 audit
    b. Stage 2 audit
2. Certification
3. Surveillance audit 1 – end year 1
4. Surveillance audit 2 – end year 2
5. Recertification audit – end year 3

The stage 1 audit shall be performed

a) to audit the client's management system documentation;
b) to evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;
c) to review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;
d) to collect necessary information regarding the scope of the management system, processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. quality, legal aspects of the client's operation, associated risks, etc.);
e) to review the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit;
f) to provide a focus for planning the stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects;
g) to evaluate if the internal audits and management review are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the stage 2 audit.

The purpose of the stage 2 audit is to evaluate the implementation, including (design) effectiveness, of the client's management system. The stage 2 audit shall take place at the site(s) of the client. It shall include at least the following:

a) information and evidence about conformity to all requirements of the applicable management system standard or other normative document;
b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);
c) the client's management system and performance as regards legal compliance;
d) operational control of the client's processes;
e) internal auditing and management review;
f) management responsibility for the client's policies;
g) links between the normative requirements, policy, performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document), any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

The recertification audit shall include an on-site audit that addresses the following:

a) the effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification;
b) demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance;
c) whether the operation of the certified management system contributes to the achievement of the organization's policy and objectives.

A recertification audit shall be planned and conducted to evaluate the continued fulfilment of all of the requirements of the relevant management system standard or other normative document. The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the

management system as a whole, and its continued relevance and applicability for the scope of certification.

3.3 Reporting

ISO/IEC 17021:2015 specifies that the Certification Body shall provide certification documents to the certified client by any means it chooses. Usually the Certification Body will issue a short form report (certificate).

According to the standard, the certification document(s) shall (from our perspective: must) identify the following:

a) the name and geographic location of each client whose management system is certified (or the geographic location of the headquarters and any sites within the scope of a multi-site certification);
b) the dates of granting, extending or renewing certification;
c) the expiry date or recertification due date consistent with the recertification cycle;
d) a unique identification code;
e) the standard and/or other normative document, including issue number and/or revision, used for audit of the certified client;
f) the scope of certification with respect to product (including service), process, etc., as applicable at each site;
g) the name, address and certification mark of the certification body; other marks (e.g. accreditation symbol) may be used provided they are not misleading or ambiguous;
h) any other information required by the standard and/or other normative document used for certification;
i) in the event of issuing any revised certification documents, a means to distinguish the revised documents from any prior obsolete documents.

For the purpose of issuing an EU Cybersecurity Certificate for Cloud Services, the conformity assessment body must issue a long form report including all elements (a up to including g) listed above. In addition, the report should also contain a description of the subservices used/included in providing the cloud service, the sub service providers involved, and identification of EU Cybersecurity Certificates issued for these subservices. The long form report should also contain all significant findings resulting from both the stage 1 and 2 audits. The long form report will be sent to the National Cybersecurity Certification Authority.

3.4 Certification

The long form report will form the basis for the issuance of the EU Cybersecurity Certificate for Cloud Services. This will be done either by the accredited conformity assessment body or the National Cybersecurity Certification Authority in accordance with Article 56 of the Cybersecurity Act:

Table 6. ISO based conformity assessment: Issuer of the certificate vs. Assurance level. Proposal.

Issuer of the certificate	Assurance level
Conformity Assessment body	Basic, substantial

Issuer of the certificate	Assurance level
National Cybersecurity Certification Authority	Basic, substantial, high

All certificates will be sent to both the National Cybersecurity Certification Authority and ENISA subsequent to Article 56 of the EUCA.

Before issuing the certificate, the issuer should verify that the whole service process is covered by valid long form reports or EU Cybersecurity Certificates.

3.5 Monitoring

The National Cybersecurity Certification Authority will maintain a register of all EU Cybersecurity Certificates issued in its jurisdiction. This register will indicate the name of the CSP, the name of the service, the date of issuance of the EU Cybersecurity Certificate, the expiration date of the validity of the Certificate and the name of the issuer. Through the register, access will be provided to the certificate itself.

4 ISAE based conformity assessment

4.1 Introduction

The International Audit and Assurance Standards Board (IAASB) of the International Federation of Accountants (IFAC) provides for a conformity assessment approach using the International Standards for Assurance Engagements (ISAE).

An assurance engagement is an engagement in which an assurance provider expresses a conclusion designed to enhance the degree of confidence of the intended users, other than the responsible party (the CSP), about the outcome of the evaluation or measurement of a subject matter (the statement of the CSP about the service, process or product) against criteria (the set of pre-defined control objectives and related measures - Annex 1). This engagement is executed in accordance with the International Standard on Assurance Engagements (ISAE) 3000/3402 as issued by the International Auditing and Assurance Standards Board (IAASB) of the International Federation of Accountants (IFAC).

ISAE forms part of a set of standards and guidelines issued by IAASB addressing audit, quality control, review, other assurance, and related services engagements. Amongst them are the global auditing standards used for auditing the financial statements of companies and organizations all over the world. These standards are adopted and translated by IFAC member bodies who in most cases are the national audit standard setting bodies that act as Accreditation Bodies for professional accountants and auditors and the organizations they belong to. The standards may only be applied by professional accountants and auditors that are recognized by IFAC member bodies based upon their education and experience.

Auditor competence in relation to performing conformity assessments with respect to CSPs is extremely important. Most professional accountants will not be able to fully understand all aspects of cloud service provision for the execution of CSP conformity assessments only specialized IT auditors like ISACA's Certified Information Systems Auditors (CISA) or NOREA's Registered IT Auditors (RE) will qualify.

4.2 Type 1 vs type 2

The ISAE standards differentiate between type 1 and type 2 assessments. A type 1 assessment is aimed at the design and implementation at a specified date whereas a type 2 assessment is aimed at the design, implementation and operating effectiveness over a specified period in the past.

In accordance with Standard ISAE 3402 the objectives of the auditor for the purpose of issuing an EU Cybersecurity Certificate for Cloud Services are:

(a) To obtain reasonable assurance about whether, in all material respects, based on suitable criteria:

i. The CSP's description of its system fairly presents the system as designed and implemented throughout the specified period (or in the case of a type 1 report, as at a specified date);

ii. The controls related to the control objectives stated in the CSP's description (Milestone 1) of its system were suitably designed throughout the specified period (or in the case of a type 1 report, as at a specified date);

iii. Where included in the scope of the engagement, the controls operated effectively to provide reasonable assurance that the control objectives stated in the CSP's description of its system was achieved throughout the specified period (type 2 only).

(b) To report on the matters in (a) above in accordance with the auditor's findings.

4.3 Scope

Under the ISAE 3402 standard the CSP must identify the subservice providers and the contributed services as a minimum requirement. The CSP and the auditor have the option to include the subservice organization in the scope of their report (inclusive method) or specifically exclude them from the scope (carve out method). If the carve out method is used, the individual conformity assessments of the various subservice providers need to be assessed separately in conjunction with the cloud service assurance report provided by the CSP.

4.4 Reporting

The assurance provider report is a long form report intended for use by a knowledgeable auditor (auditor-to-auditor report). For the purpose of issuing an EU Cybersecurity Certificate for Cloud Services the format described in ISAE 3402 must be followed (see Annex 4 as well):

- Type 1 Report: reports on the description and design of controls at a service organization and comprises of
  - The CSP's description of its system;
  - A written assertion by the CSP that, in all material respects, and based on suitable criteria:
    a. The description fairly presents the CSP's system as designed and implemented as at the specified date in accordance with the pre-defined framework;
    b. The controls related to the control objectives stated in the CSP's description of its system were suitably designed as at the specified date; and
  - An auditor's assurance report that conveys reasonable assurance about the matters in a.–b. above, including the way of gathering evidence.

- Type 2 Report: reports on the description, design and operating effectiveness of controls at a service organization and comprises of:
  - The CSP's description of its system;
  - A written assertion by the CSP that, in all material respects, and based on suitable criteria:
    a. The description fairly presents the service organization's system as designed and implemented throughout the specified period;
    b. The controls related to the control objectives (Milestone 1) stated in the service organization's description of its system were suitably designed throughout the specified period; and
    c. The controls related to the control objectives stated in the service organization's description of its system operated effectively throughout the specified period; and
  - A service auditor's assurance report that:
    a. Conveys reasonable assurance about the matters in a.–c. above; and
    b. Includes a description of the tests of controls and the results thereof.

4.5 Certification

The long form report will form the basis for the issuance of the EU Cybersecurity Certificate for Cloud Services. This will be done either by the accredited conformity assessment body or the National Cybersecurity Certification Authority in accordance with Article 56 of the EUCA:

Table 7. ISAE based conformity assessment: Issuer of the certificate vs. Assurance level. Proposal.

Issuer of the certificate	Assurance level
Conformity Assessment body	Basic, substantial
National Cybersecurity Certification Authority	Basic, substantial, high

All certificates will be sent to both the National Cybersecurity Certification Authority and ENISA subsequent to Article 56 of the EUCA.

Before issuing the certificate, the issuer should verify that the whole service process is covered by valid assurance reports or EU Cybersecurity Certificates.

5 Comparison of conformity assessment methodologies

5.1 Relevant elements for certification related to assurance reporting

Next, a comparison of relevant elements for assurance reporting is shown.

Table 8. Relevant elements for certification related to assurance reporting

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
Reporting cycle	3 years cycle approach Initial audit in 2 stages, 2 years of surveillance audits completed by recertification.	Yes, every year.	Valid for a defined and communicated period in time (for example one year) and must be withdrawn by the cloud provider if it is no longer accurate.
Timeframe	One point of audit as audit focus on design.	Audit period covers typically 6-12-months period.	A snapshot of a period.
Criteria (i.e. whether our Milestone 1 criteria are sufficient to allow the certification scheme to be applied)	ISO Certification requires the use the ISO security schemes., e.g. 27xxx series. Milestone 1 scheme is an EU defined cloud security framework. The related EU certificate is based upon the ISO approach as described in section 4 of this annex.	Yes, all standards (including Milestone 1 criteria) or frameworks are allowed to be used in ISAE 3402 audit as long the criteria exhibit the following characteristics: a. Relevance. b. Completeness. c. Reliability. d. Neutrality. e. Understandability.	No criteria are set but can be determined. Criteria must be double checked in the course of Milestone 3.

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
Guidance for audit procedure.	ISO 19011 describing the details and is a design review.	Yes, ISAE 3402 describes the nature, timing and extent of the audit procedures for design and operating effectiveness of controls.	Guidance must be defined in correlation with the criteria of the scheme (probably part of Milestone 3).
Reporting and evidence	Certificate, 1 page available for all users. Consider the use of a long form report as described in the next column (3402), which includes the procedures performed by the auditor, the evidence gathered, and the conclusions drawn for each of the criteria, resulting in an overall statement of conformity.	Report containing the auditor's opinion, management's assertion, description of system and controls, complementary user entity controls, performed tests of controls and their results. The report is available for IT – auditors, CPAs, and users of the service that have sufficient understanding to interpret the report. A certificate based on one or more reports would make the results available for all users.	The result of the EBCA is made publicly available, and the assessment report is available to the third party (but not necessarily to customers or other third parties).

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
Subcontractors.	Subcontractors are not necessarily included in the scope of an ISO certificate. However, a CSP may rely on the ISO certificate of its subcontractors. Subcontractors (or carve-outs of subcontractors) must be disclosed by the CSP to customers or other relying parties in the same manner as its certificate.	Relevant subcontractors are described in the report. They can either be included in the scope of the report or carved-out.	The CSP can rely on existing certificates or attestations from its subcontractors, or on -assessment statements within the same or equivalent schemes from its subcontractors. Subcontractors (or carve-outs of subcontractors) must be disclosed by the CSP to customers or other relying parties.

5.2 Relevant elements of CAM related to the individual performer and control system

Next, a comparison of the elements of conformity assessment methods related to the individual performer and control system is shown.

Table 9. Comparison of the elements of conformity assessment methods related to the individual performer and control system

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
Independence the more independent (from the CSP) the party who performs the assessment is, the more trustworthy and credible the conclusion or statement will be.	Yes, ISO 17065/17021 describe independence in the principles.	The Code of Ethics for Professional Accountants issued by the (IESBA) requires the auditor to be independent.	A credibility check of the self-assessment is done by an independent third party. For this purpose, a monitoring body/bodies has /have to be appointed (e.g. by national or European agency)
Competency / Expertise the performer of the assessment needs to be competent (expertise, skills and experience) to be able to execute the work to be done	Yes, for accredited auditors only in accordance with ISO/IEC 17021, e.g. appropriate knowledge as for example described under 3402 approach	Required competence conducting an ISAE audit: - Knowledge of the relevant industry; - An understanding of information technology and systems; - 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	Skills should be appropriate for the information security assessment criteria of the scheme (but no evidence is necessarily available). Appropriate skills as for example described under 3402 approach.

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
Professional Standards the performer of the assessment needs to adhere to the applicable professional standards	Yes, ISO 17065/17021 describes independence in the principles.	Professional standards addressing audit, quality control, review, other assurance, and related services.	No standardized method.
Code of Conduct the performer of the assessment needs to adhere to a professional code of conduct issued by the recognized body	Auditors should exhibit professional behaviour during the performance of audit activities. No specific Code of Conduct is available for the auditor. The guidelines from ISO/IEC 19011:2011, Clause 7.2.3.2 apply. (7.2.3.2 parts A.B.C etc.)	Yes, the IT - auditors require to comply with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA), which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.	A statement of ethical principles should be made available to relying parties upon request.
Qualification and Accreditation the performer of the assessment needs to be qualified by being a member of a recognized body of IT-auditors, Internal auditors, or external auditors or being a	National accreditation body will accredit certification body against ISO 17065/17021.	An-IT auditor, or national equivalent are governed by law or guidelines set by the professional organization of the member states of IFAC.	The auditor within the cloud provider is not necessarily accredited. However, the credibility check shall be done by an accredited independent third party.

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
partner in a recognized audit firm. the performer of the assessment needs to have an accreditation issued by a recognized body of IT-auditors, Internal auditors or External Auditors, or issued by a National Accreditation Body.		(e.g. Wirtschaftsprüfer-ordnung in Germany, NOREA/ NBA in the Netherlands).	
Accountability and Liability The performer of the assessment is accountable for the work performed and the report issued. The performer of the assessment can be held liable in case of negligence or bad execution caused damage	Complaints are handled between the certification body and the client, ISO 17065, no disciplinary law in ISO defined.	Disciplinary law is applicable for the IT – auditor and audit firm. It could be used (option) to be legally binding for the CSP including it into the contract.	The statement made by the CSP must be legally binding for the CSP (and may be a part of a contractual framework or SLA) signed by a legal representative of the CSP who assumes responsibility and liability through the CSP for the accuracy of the assessment.
Monitoring and Supervision the performer of the assessment needs to have supervision, being		An auditor is always a member of firm that is subject to International Standard on Quality Control (ISQC's) which stipulates the rules for the	As already mentioned in A., an appointed monitoring body should supervise the desk review processes

Relevant elements to distinguish the three methods related to the output.	**Third party assessment based on ISO17065/17021** [17] **and ISO19011** [32]	**Third party assessment based on ISAE3402 Type 2** [28]	**Evidence based conformity assessment (*).** (*) As there is no existing methodology in place elements are proposed on an existing approach used by Trusted Cloud in Germany
monitored in a systematic way and periodically reviewed by his organization and/or recognized body.		responsibility to maintain a system of quality control for monitoring regarding the firm responsibility. Part of these systems are control reviewers	

6 Background information

6.1 Characteristics of performing an audit

The following elements are characterizing and audit:

- A three-party relationship:
  - o the responsible party (the CSP),
  - o the intended or interested users, i.e. the cloud customer,
  - o the practitioner or assurance provider (Conformity Assessment Body);
- An appropriate subject matter: this is the statement (see Annex 4) and the supporting documentation or evidence of the CSP that his service, product or process is in accordance with the predefined security framework;
- Suitable criteria: the predefined security framework of control objectives, criteria and related measures (i.e. as defined in Milestone 1, Annex 1);

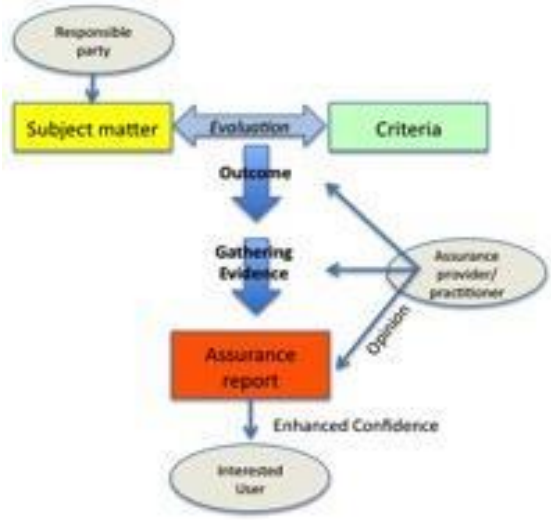

Figure 13. Process of an audit

- Evidence: the evidence gathered by the assurance provider to validate the statement of the CSP;
- Opinion [Assurance report]: the report on the conformity assessment issued by the Conformity Assessment Body or Audit Firm.

Annex 3 – Glossary

1 Cybersecurity Act Article 2 Definitions

The following terms are defined in Article 2 of the Cybersecurity Act [33]. Their meaning in this document is aligned with the definition of this regulation. They are copied in this document for readability issues but are publicly available in [33]

1. **'cybersecurity'** means all activities necessary to protect the network and information systems, their users, and affected persons from cyber threats;
2. **'network and information system'** means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148 [34];
3. **'national strategy on the security of network and information systems'** means a national strategy on the security of network and information systems as defined in point (3) of Article 4 of Directive (EU) 2016/1148 [34];
4. **'operator of essential services'** means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148 [34];
5. **'digital service provider'** means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148 [34];
6. **'incident'** means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148 [34];
7. **'incident handling'** means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148 [34];
8. **'cyber threat'** means any potential circumstance, event or action that may damage, disrupt or otherwise adversely impact network and information systems, their users and affected persons.
9.
    a. **'European cybersecurity certification scheme'** means the comprehensive set, defined at Union level, of rules, technical requirements, standards and procedures applying to the certification or conformity assessment of Information and Communication Technology (ICT) products, services and processes falling under the scope of that specific scheme;
    b. **'national cybersecurity certification scheme'** means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority applying to the certification or conformity assessment of ICT products, services and processes falling under the scope of that specific scheme;
10. **'European cybersecurity certificate'** means a document issued by the relevant body attesting that a given ICT product, service or process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;
11.
    a. **'ICT product'** means any element or group of elements of network and information systems;
    b. **'ICT service'** means any service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

c. **'ICT process'** means any set of activities performed to design, develop, deliver and maintain an ICT product or service;

12. **'accreditation'** means accreditation as defined in point (10), Article 2 of Regulation (EC) No 765/2008 [26];
13. **'national accreditation body'** means a national accreditation body as defined in point (11), Article 2 of Regulation (EC) No 765/2008 [26];
14. **'conformity assessment'** means conformity assessment as defined in point (12), Article 2 of Regulation (EC) No 765/2008 [26];
15. **'conformity assessment body'** means conformity assessment body as defined in point (13), Article 2 of Regulation (EC) No 765/2008 [26];
16.
    a. **'standard'** means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012 [35],
    b. **'technical specification'** means a document that prescribes technical requirements to be fulfilled by ICT process, product, service or conformity assessment procedures;
    c. **'assurance level'** means a ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme and states at what level it has been evaluated; the assurance level does not measure the security of an ICT process, product or service themselves.
17. **'self-assessment'** means an action carried out by the manufacturer or provider of ICT services, products or processes which evaluates the fulfilment of the requirements set in a European cybersecurity certification scheme.

2 CSPCERT General Terms

This section of the Annex 4 Glossary aims to present the terms related to cloud computing and certification.

Each term is accompanied by a definition as well as the source of such definition.

Audit: 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 communicating the results to interested users [36].

Audit scope: extent and limits of an audit [37].

Authentication: process that ensures the recognition that an entity (person, organization or system) is who is claims to be [37].

Assurance - a systematic process in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria. The outcome of the evaluation or measurement of a subject matter is the information that results from applying the criteria [27]

Authentication: process that ensures the recognition that an entity (person, organization or system) is who is claims to be [37].

Availability: process of being accessible and usable when demanded by an authorized party [37].

Certification: formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certification indicating conformance [30].

Cloud Computing: model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models [38]. It allows therefore storing, processing and use of data on remotely located computers accessed over the internet [39]

Cloud Governance: It can be external or internal. External governance involves an agreement between the cloud service consumer and the cloud service provider concerning the use of cloud services by the cloud service consumer. The internal cloud governance is the application of design-time and run-time policies to ensure the cloud computing based solutions are designed and implemented, and cloud computing based services are delivered according to the specified expectations [40].

Cloud Service: any IT service (e.g. resource, database, virtual machine, application and so on) that are provisioned and accessed from a cloud service provider.

Cloud Service Agreement: documented agreement between the cloud service provider and the cloud service customer that governs the covered service [41]**.**

Cloud Service Level Agreement (CSLA): part of the cloud service agreement that includes the cloud service level objectives and cloud service qualitative objectives for the covered cloud services [41]**.**

Cloud Service Level Objective (CSLO): commitment of a cloud service provider for a specific, quantitative characteristic of a cloud service the value follows the interval scale or a ratio scale [41]**.**

Cloud Service Consumer (CSC): organization or individual that has a business relationship, and therefore a contract, to use the IT resources provided by a cloud service provider [42].

Cloud Service Provider: (CSP) organization that makes IT resources and services available. A Cloud Service Provider must ensure the delivery and maintenance of its services to the cloud service customer [42].

Conformity: fulfilment of a requirement [37].

Conformity Assessment Body: an organization accredited by the national accreditation body [30]**.**

Corrective action: action taken to eliminate the cause of a non-conformity and to prevent occurrence [37].

Cybersecurity Certification: formal evaluation to attest that the ICT products and services comply with the cybersecurity requirements specified in the corresponding scheme [30].

Disaster recovery: ability of an ICT system to support its critical business functions to an acceptable level within a predetermined period of the time following a disaster [41].

Failure notification policy: set of rules and procedures specifying the processes by which the cloud service customer can notify the cloud service provider of a service outage and by which the cloud service provider can notify the cloud service customer that a service outage has occurred [41].

Governance: means by which the provision and use of a cloud service are controlled and extended. [42]

Governance of Information Security: system by which the information security activities of an organization are directed and controlled [37].

Incident: any event having an actual adverse effect on the security of network and information systems [43]. This event can actually or potentially jeopardize the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies [9].

Incident management and incident handling: set of procedures supporting the detection, analysis and containment of an incident and the response thereto [43], assuring a consistent and comprehensive approach regarding the monitoring, recording, assessment, communication and escalation of security incidents [4, 25].

Information processing facilities: location housing any information processing system, service or infrastructure [37].

Information security: preservation of confidentiality, integrity and availability of information [37].

Information security event: an identified occurrence of a system, network or service state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant [37].

Information security incident: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations of the organization or of threatening information security [3] [37].

Information System Security Audit Service Provider: Audit service provider for information system security. It is said to be approved if an approval entity has certified its compliance with the Requirements reference document for information system security audit service providers [3].

Information security management system: set of policies and procedures for systematically managing an organization's sensitive data. It aims to preserve the confidentiality, integration and availability of information by applying a risk management process in order to ensure confidence to interest parties that risks are adequately managed [44].

Information security-related risks: risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the potential adverse impacts to organizational operations and assets, individuals, and other organizations, public or private. [9]**.**

Information system: Organized set of resources (hardware, software, staff, data, and procedures) that allow information to be processed and circulated [3].

Interoperability: ability of two or more systems or applications to exchange information and to mutually use this information. In the case of cloud computing, interoperability is the capability of public, private, hybrid cloud service providers to understand each other's' interfaces, configuration, authentication and authorization mechanisms, and so on, so as to be able to cooperate with each other [45].

Integrity: accuracy and completeness [37].

IT Security policy: documentation of IT security decisions [46]

Non-conformity: a not fulfilment of a requirement [37]**.**

Portability is the ability for a cloud service consumer (CSC) to move their data or their applications between two different cloud services at low cost with minimal disruption [42]

Personally Identifiable Information: any information that can be used to a) identify the personally identifiable information (PII) principal to whom such information relates to, or b) is or might be directly or indirectly linked to a PII principal [47].

Policy: Intentions and orientations of an organization such as formalized by its management [3] [37]. The representation of rules or relationships that makes it possible to determine if a requested access should be allowed, given the values of the attributes of the subject, object, and possibly environment conditions [48].

Resiliency: ability of a system to provide and maintain an acceptable level of service when faults occur, independently if they are unintentional, intentional or naturally caused), affecting the normal operation [40]**.**

Requirement: need that has to be fulfilled. It can be mandatory or optional [37]**.**

Risk: Effect of an uncertainty as to achieving a set of specific objectives. This is expressed in terms of a combination of consequences of an event and of its likelihood [3] [37]. Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems [43].

Risk assessment: process of identifying, analyzing and evaluating a risk [37].

Risk management process: systematic application of policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [37].

Security control: a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements [9].

Security control assessment: testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization [9].

Security control effectiveness: the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies [9]**.**

Security control objective: statement describing what it is to be achieved as a result of implementing a control [37].

Security incident: see Incident.

Security of an information system: All of the technical and non-technical controls that make it possible for an information system to manage the availability, integrity or confidentiality of the data that is processed or transmitted and the related services that these systems provide or make available [3].

Security measure: Measure that modifies the likelihood or the severity of a risk. It includes the policy, procedures, guidelines, and the organizational practices or structures, and can be of an administrative, technical, managerial or legal nature [3].

Service Level Agreement (SLA): see Cloud Service Level Agreement.

Service Level Objective (SLO): see Cloud Service Level Objective.

Security policy: A set of criteria for the provision of security services [9].

System integrity: state of a system in which the intended functions are performing in an adequate manner, that is, without the system being degraded or interrupted.

Technical infrastructure: All of the hardware and software components required for the making available of resources allocated to the demand (virtualized or not). This basis allows for the accomplishing of the service within the framework of an IaaS service or is used as a basis for building the service in the other cases [3].

Tenant: one or more cloud service consumer sharing access to a set of resources, virtual or physical [42].

Threat: Potential cause of an undesirable incident that can harm a system or organization [3] [37].

Virtualized resources: Abstraction of the hardware resources of a system (CPU, RAM, etc.) which are made available by the technical infrastructure [3].

Vulnerability: Weakness of property or control that can be exploited by one or more threats [3] [37] [9].

Annex 4 – Template Report CSP Management Assessment [8]

This template is to be used by the CSP's to provide information to:

- The review body in case of Evidence Based Self-Assessment;
- The conformity assessment body to be able to execute their conformity assessment.

It also provides evidence of the self-assessment process executed by the management of the CSP.

The structure of this template report follows the format of ISAE 3402 (in the US SSAE 16 / AT section 801, referred to as SOC).

1. Identification

[Name of the CSP]

[Short description of the service]

[As of date of the report in case of a type I report]

or [The reporting period in case of a type II report]

2. CSP's Conformity Statement

This is a written statement by the management of the CSP.

This statement includes that, in all material respects:

- Management's description of the service delivery fairly presents the CSP organization's system that was designed and implemented as of a specific date or throughout the specified period (type I respectively type II), based on the EU framework on Cloud Security

Note: reference to the control framework as defined by the EU i.e. the Milestone 1 document.

- The controls stated in management's description of the CSP organization's system were suitably designed to meet the applicable security objectives as of a specific date or throughout the specified period (type I respectively type II);
- The controls stated in management's description of the CSP organization's system operated effectively throughout the specified period to meet the applicable control objectives (type II report)

3. CSP's description of its service

The description of the service contains the information shown in the next sections.

3.1 The types of services provided

3.2 The components of the system

A description of the components of the system used to provide the services, which are as follows:

[8] This annex is based on the NOREA Guide to ISAE 3000 Service Organization Control reports for IT Service Organisations, the Netherlands, March 2016; NOREA is the Dutch Institute for IT-Auditors.

- Infrastructure: The physical structures, IT and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunication networks);
- Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- People: The personnel involved in the governance, operation and use of a system (developers, operators, users and managers);
- Procedures: The automated and manual procedures involved in the operation of a system;
- Data: the information used and supported by a system (transaction streams, files, databases and tables).

Reference needs to be made to underlying documentation and executed procedures.

3.3 The boundaries or aspects of the system covered by the description

Explain here the boundaries of the system under certification

3.4 Subservices

For information provided to, or received from, subservice organizations and other parties:

- how the information is provided or received and the role of the subservice organizations and other parties;
- the procedures the CSP performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

If the CSP presents the subservice organization using the carve-out method a description is required of:

1. the nature of the services provided by the subservice organization;
2. each of the applicable control objectives that are intended to be met by controls at the subservice organization, alone or in combination with controls at the CSP, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.

3.5 Framework

The applicable framework of control objectives and measures (i.e. Milestone 1) and the related controls designed to meet those objectives, including, as applicable, the following:

- Complementary user entity controls contemplated in the design of the CSP organization's system
- When the inclusive method is used to present a subservice organization, controls at the subservice organization.

3.6 Other

In addition to these specific requirements that are unique for IT service organizations, the following relevant aspects of the control environment are included:

- Control Environment (i.e., management philosophy, security management, security policies, personnel security, physical security and environmental controls, system monitoring, problem management, data back-up and recovery, system account management));
- Risk Assessment process;

- Information and Communication systems;
- Monitoring of controls.

4. The control objectives, related controls and tests of controls

This section typically contains the control objectives, the CSP's control activity, the test approach, and the test results per control, including the supporting documentation.

The control objectives are defined by the EU framework, the control activities supporting the criteria are those of the CSP, and the test approach and test results are those of the auditor representing the conformity assessment body. Note that including the description of tests of controls and the test results is part of a type II report. It is optional for type I reports to include the results of the evaluation of the suitability of the design.

5. Other information provided by the CSP

The content of this section is not pre-determined and is optional.

The CSP may wish to include this information if it is deemed appropriate. The following are examples of such information:

- Future plans for new systems applicable to the user entity or system
- A plan of approach to remediate any deficiencies noted in the report
- Responses from management for deviations identified by the auditor when such responses have not been subject to procedures by the auditor
- Other services provided by the service organization that are not included in the scope of the engagement, such as business continuity related controls

Annex 5 - Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0	27.03.2019	Initial Draft	Aurélien Leteinturier
V0.1	01.05.2019	Initial Draft. Review, addition of recommendations and minor spelling corrections.	Borja Larrumbide
V0.2	09.05.2019	Updated EUCA numbering, addition of recommendations, review and corrections with working team	William Ochs
v0.3	10.05.2019	Included as annex 1 the Milestone 1 document related to the security objectives. Minor corrections	Leire Orue-Echevarria
v0.4	16.05.2019	Output from Bonn and Paris working sessions toward final reviewable draft for primary WG.	William Ochs
v0.5	04.06.2019	Final edition of the document, ready for the final internal review	Leire Orue-Echevarria
0.6	06.06.2019	Addressed all reviewed items.	Leire Orue-Echevarria
1.0	06.06.2019	Ready for publication	Leire Orue-Echevarria
Final	07.07.2019	Final version for publication	Borja Larrumbide