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

Final Editor:	Leire Orue-Echevarria
Status-Version:	Final
Date:	06.06.2019
Distribution level (CO, PU):	Public

Editor(s)	Aurelien Leteinturier; William Ochs; Bert Tuinsma; Borja Larrumbide; Leire Orue-Echevarria; Clemens Doubrava, Tom Vreeburg; Thomas Niessen; Hans Graux
Contributor(s)	Saurabh Ghelani; Daniele Catteddu
CSPCERT 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 an 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 3000, 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 self-regulatory 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 product, service or process. 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/IEC 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 product, service or process to a set of criteria. As both the procedures (according to Article 52 of the EUCA ~~Cybersecurity Act~~) 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 products/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 CSP 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~~European Union~~ in accordance with the EUCA~~Cybersecurity Act~~. Apart from the bodies and regulations mentioned in the EUCA~~European Cybersecurity Act~~, 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~~European Cybersecurity Act~~.
- 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 Cybersecurity Act 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 WG and its governance documents.

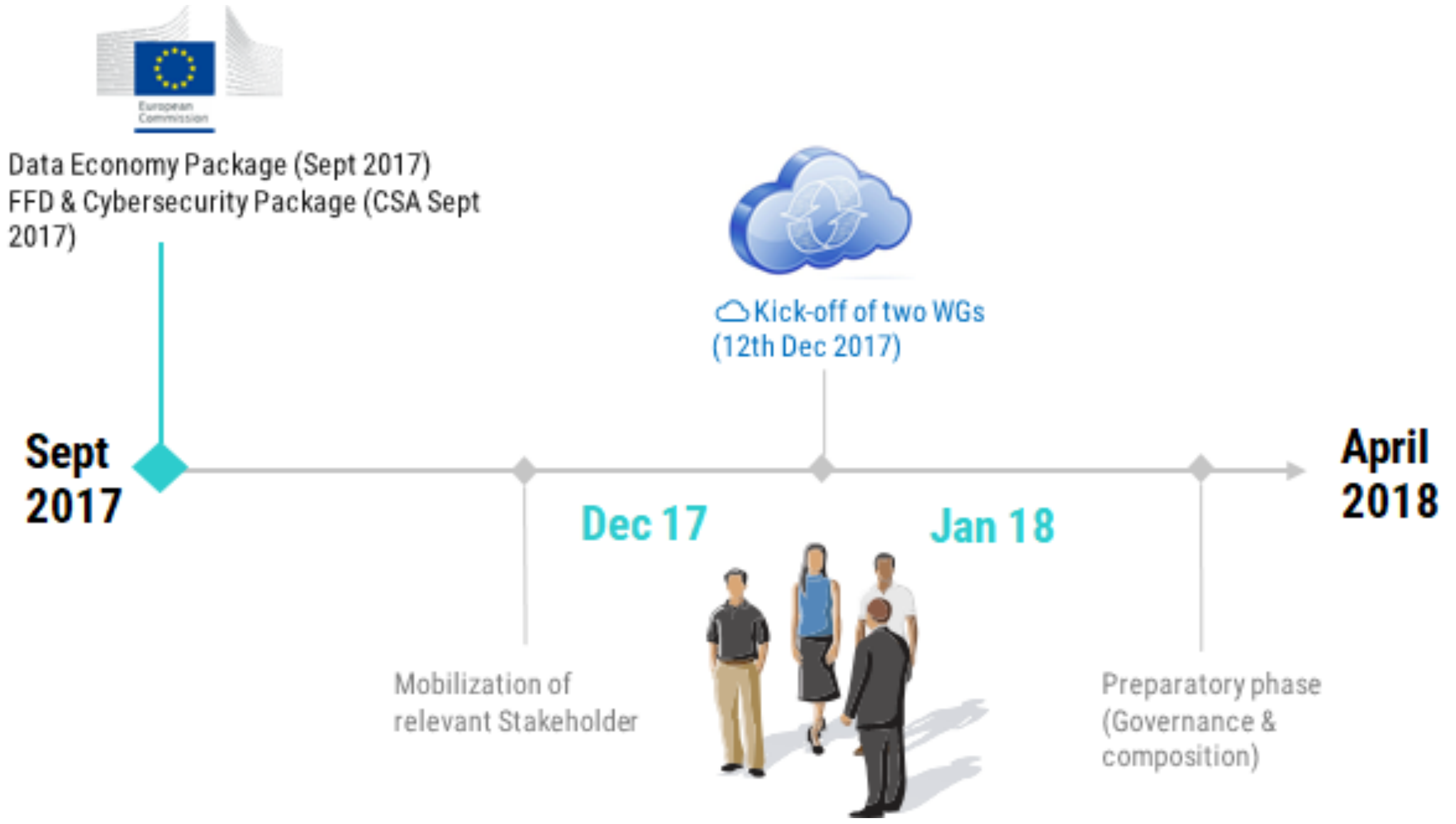
Data Economy Package (Sept 2017)
FFD & Cybersecurity Package (CSA Sept 2017)
Kick-off of two WGs (12th Dec 2017)
Sept 2017
Dec 17
Jan 18
April 2018
Mobilization of relevant Stakeholder
Preparatory phase (Governance & composition)

Figure 1. CSPCERT WG timeline

According to the Cybersecurity Act, the European Commission can request ENISA ~~(European Union Agency for Network and Information Security)~~ 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.

[1] The most recent version of the Cybersecurity Act is available at the time of drafting at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2019-0151#BKMD-20

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 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.

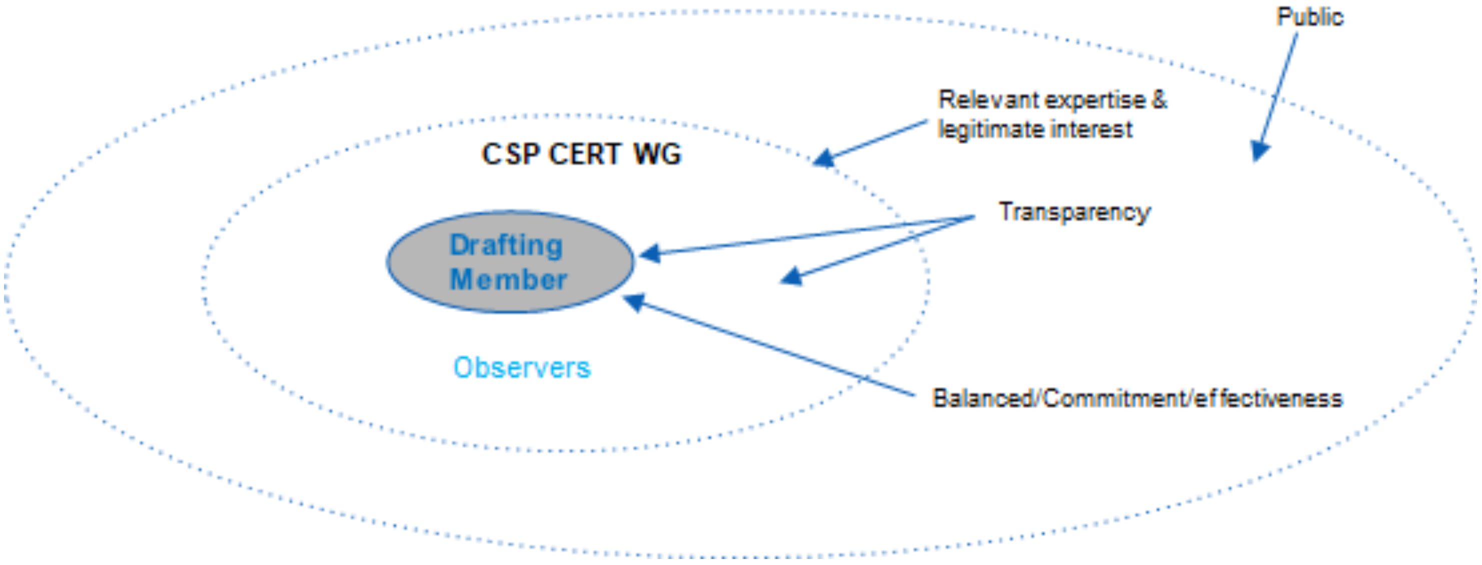
Public
Relevant expertise & legitimate interest
CSP CERT WG
Drafting Member
Transparency
Observers
Balanced/Commitment/effectiveness

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.

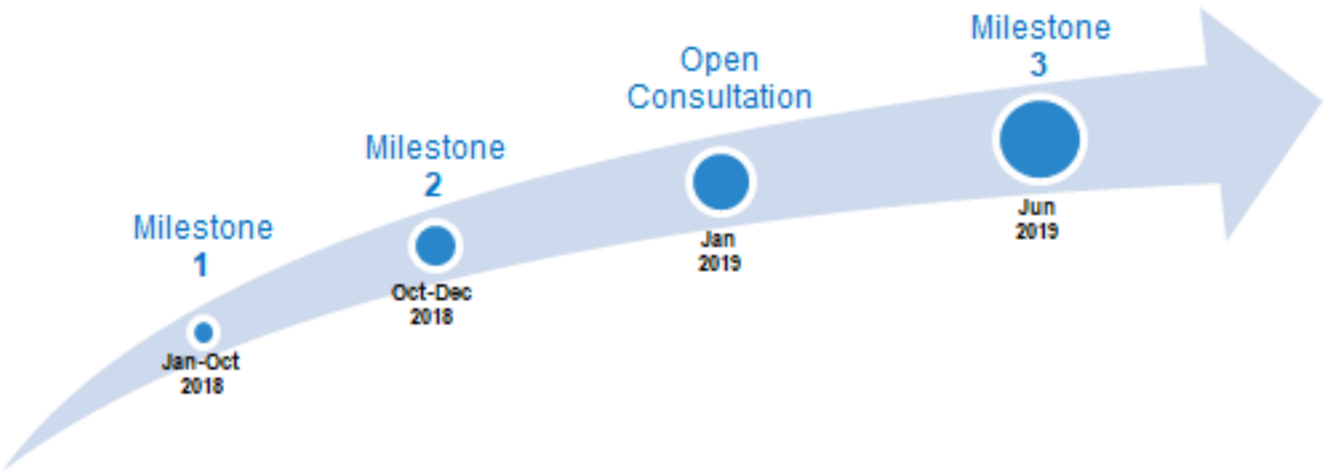

Figure 3. CSPCERT WG Milestones and Open consultation dates

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: it 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~~Cybersecurity Act~~. 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: it provides a comparative analysis of the most relevant conformity assessment methodologies. This Milestone outlines the different approaches to assess conformity of a cloud ~~process, product or~~ 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): it 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. 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. 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], ~~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.~~ BSI 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 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.

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~~Cybersecurity Act~~ 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~~Cybersecurity Act~~ 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 this document provides several detailed recommendations for the implementation of those requirements from Title III of the EUCA~~Cybersecurity Act~~, 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. **Cybersecurity Act Requirements (CSAR)**: i.e. recommendations refining the high-level requirements of the Cybersecurity Act 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~~Cybersecurity Act~~ which are sufficiently detailed in the Act itself, and that are common to all certification schemes. These aspects (such as e.g. the decision-making procedure used to formally adopt the scheme) are not in scope of the CSPCERT WG activities.

The matrix below maps each article of Title III of the EUCA~~Cybersecurity Act~~ to the corresponding recommendations stated in the paragraphs of this document:

Table 1. Correspondence between the articles of the 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 corresponding European certification schemes after their adoption.			X
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 applicable to the service scope (e.g. IaaS, PaaS, SaaS, 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~~Cybersecurity Act~~. 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 should be a guide to ensure that all these objectives are fulfilled regarding a certain assurance level.

The EUCA~~Cybersecurity Act~~ 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~~Cybersecurity Act~~ 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~~Cybersecurity Act~~, broken down into bullet points from A to J. Recommendations made by the CSPCERT WG are included in grey celled tables.

A European cybersecurity certification scheme shall be so designed as 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 already defined in Milestone 1 document presented in Annex 1 (e.g. section 3.4 'identity and access management' and section 3.5 'cryptography and key management') extending them not only to include people but also programmes, machines, APIs and associated technology.

Justification: The security objectives elicited in the Milestone 1 document present the methodology followed by the CSPCERT WG, it shows the elicited security objectives and reveals the high-level gap analysis between 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 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.

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

REC2: Products and services should be updated at a 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 product 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 those already defined in Milestone 1 document presented in Annex 1 (e.g. section 3.7 'Operational security' and more specifically OS.6)

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

(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 to meet this requirement in the vetted Milestone 1 documentation effort conducted by CSPCERT WG.

(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 to meet this requirement in the vetted Milestone 1 documentation effort conducted by CSPCERT WG.

(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 to meet this requirement in the vetted Milestone 1 documentation effort conducted by CSPCERT WG.

(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 to meet this requirement in the vetted Milestone 1 documentation effort conducted by CSPCERT WG.

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) 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 offer that allow 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~~Cybersecurity Act~~. The wording from the EUCA~~Cybersecurity Act~~ 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 requirement on a particular level of certification according to the costs, the verification level and impact of a cyber incident on the cloud service. Any assurance level assigned to a qualified cloud service through the EUCA~~Cybersecurity Act~~ certification scheme should have conducted a recognized risk analysis, which would be reviewed as part of their 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.

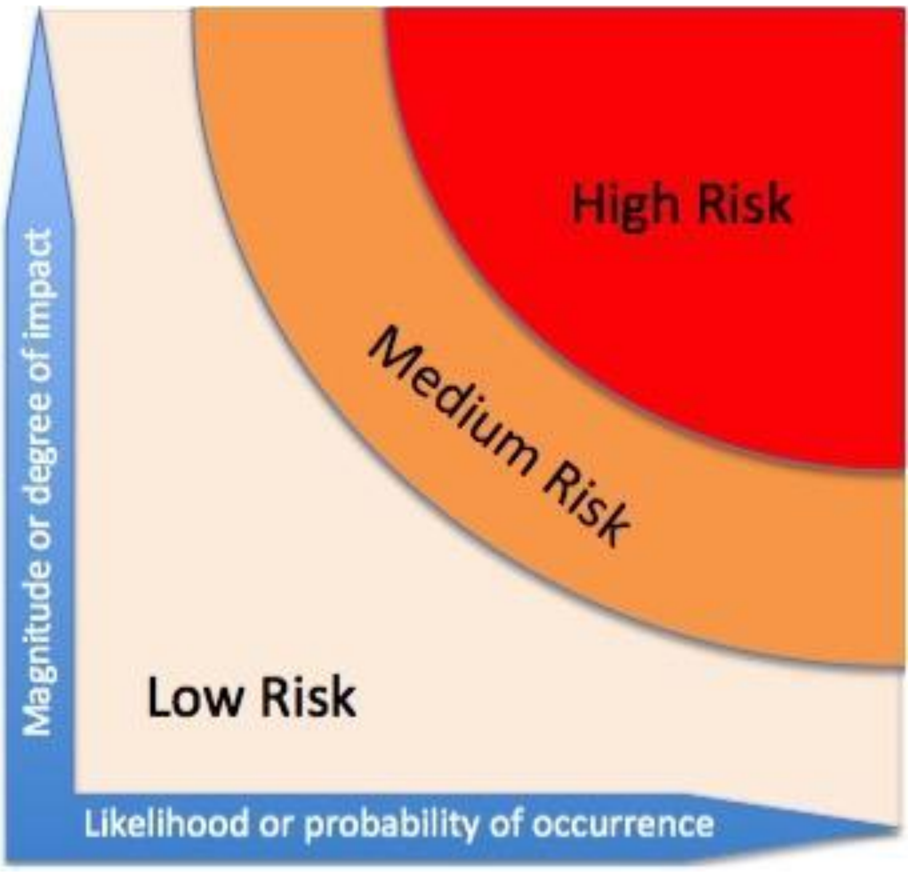
High Risk
Medium Risk
Low Risk
Magnitude or degree of impact
Likelihood or probability of occurrence

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 would disrupt it.

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

- 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 c~~C~~ertification 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 call out that there is no coverage in the EUCA for operational or unintentional disruptions of a service. The final scheme should include this dynamic such as 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 impacts.

For the cloud computing certification scheme 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 product aligns to an appropriate assurance level. 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 of course could mature over time with evolving threat landscapes.

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 that can mature over time, should be presented to the public, that addresses 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 service.

~~the free flow of non-personal data (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 [15].~~*~~The use of CCAL High certification is recommended in cases where legal data localization restrictions apply.~~*

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 risk scenarios 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	**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 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 ~~h~~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; ● 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 for deciding the assurance level that is required for their own needs. Sometimes, an assurance level can be forced through regulation for critical sectors, for example. 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.