

SURVEILLANCE
DU MARCHÉ

ACCREDITATION

CONFIANCE
NUMÉRIQUE

MÉTROLOGIE

NORMALISATION

ILNAS

Welcome
Bienvenue
Willkommen

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

06-07/10/2022, Belval

Jean-François Gillet

Project officer – *Digital Trust Department*, ILNAS

10/6/2022



EUCS

<https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>

- “EUCS” means European Cybersecurity Certification Scheme for Cloud Services
- EUCS draft version has been published on December 22nd, 2020
- 22 articles in EUCS cover article 54 from CSA (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN>)
- Additional topics and Annexes (9)
- [Webinar](#) by ENISA Lead Certification Expert Eric Vétillard on January 2021

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

Article 54 (a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;

Reference to chapter
or annex in the EUCS

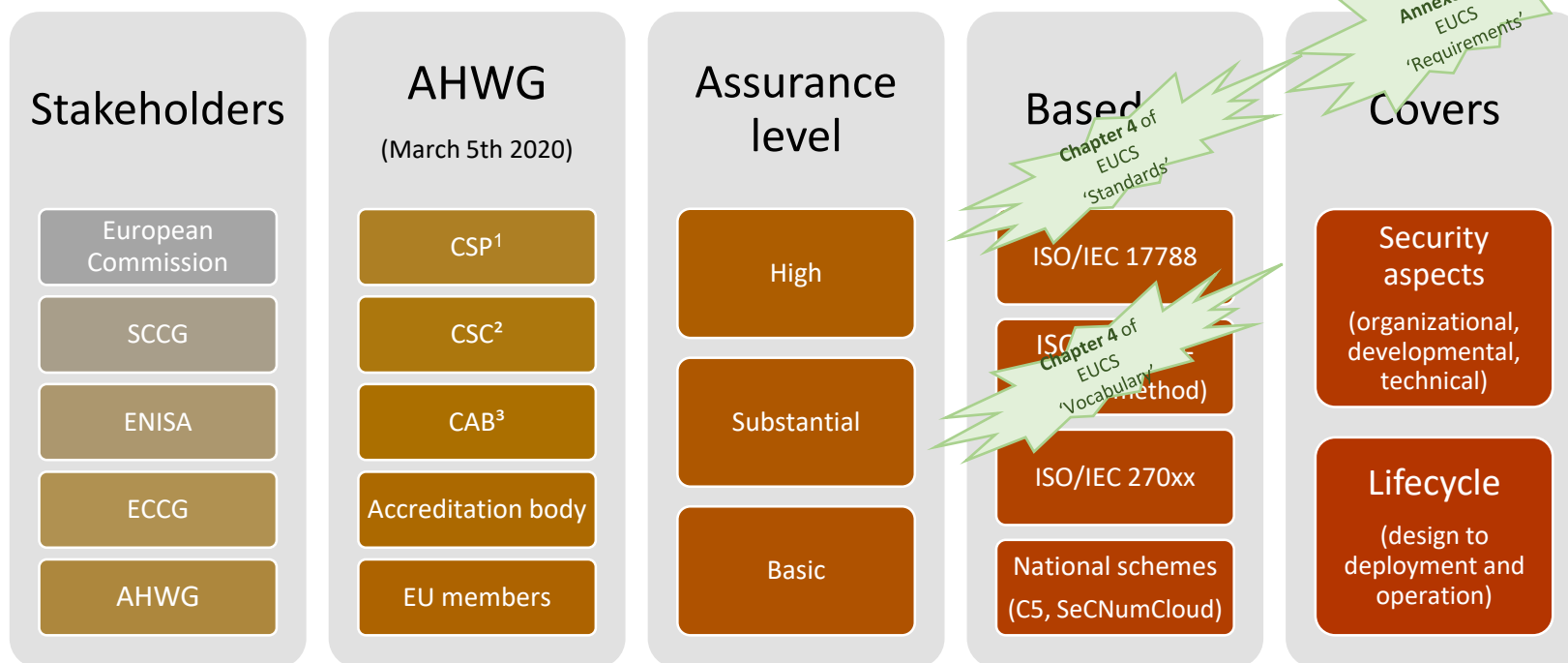
- Details

- ...
- ...
- ...
- ...
- ...
- ...
- ...
- ...

Reference the CSA

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

Article 54 (a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes covered;



¹ Cloud Service Provider : Party which makes cloud services available

² Cloud Service Customer : Party which is in a business relationship for the purpose of using cloud services

³ Conformity Assessment Body as defined in CSA article 60

Article 54 (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;

Increase security
of cloud services
(and uptake within Europe)

A scheme
harmonized at
EU level

Target audiences

- CSPs
- CSCs
- Regulators
(baseline for security)

Article 54 (d) where applicable, one or more assurance levels;

Quick review

BASIC

- Minimize the known basic risks of incidents and cyberattacks
- Evaluation: at least a review of technical documentation
- Minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources
- Evaluation consist of at least the following:

SUBSTANTIAL

a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the target correctly implements the necessary security functionalities

HIGH

- Minimize the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources
- Evaluation consist of at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the target correctly implements the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing

Annex A has the full set of security requirements and directly maps these requirements to assurance levels 'basic', 'substantial', and 'high'

Article 54 (e) an indication of whether conformity self-assessment is permitted under the scheme;

- Conformity self-assessment cannot be used for 'basic' assurance level in the current scheme

Article 54 (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;

Security objectives

- Explicit mapping of [Annex A](#) requirements to Art. 51 objectives

Evaluation

- [Annex B](#) defines an overall evaluation approach
- **Annex C** gives specifics for ‘substantial’ and ‘high’. Inspired by standards. “Reasonable assurance” is achieved
- **Annex D** gives specifics for ‘basic’. Evidence-based. “Limited assurance” is achieved. Based only on CSP-provided evidence

Article 54 (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;

[Annex F](#) provides a certification mandatory application template format



Evidence in all cases includes (ie):

- Policies and procedures (possibly evidence of use)
- Records on subservices

See also the specific Annexes (B in all cases, C and D depending on the assurance level)

Article 54 (i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

- A framework to easily identify the certificate, for a variety of purposes
- While it is valid only

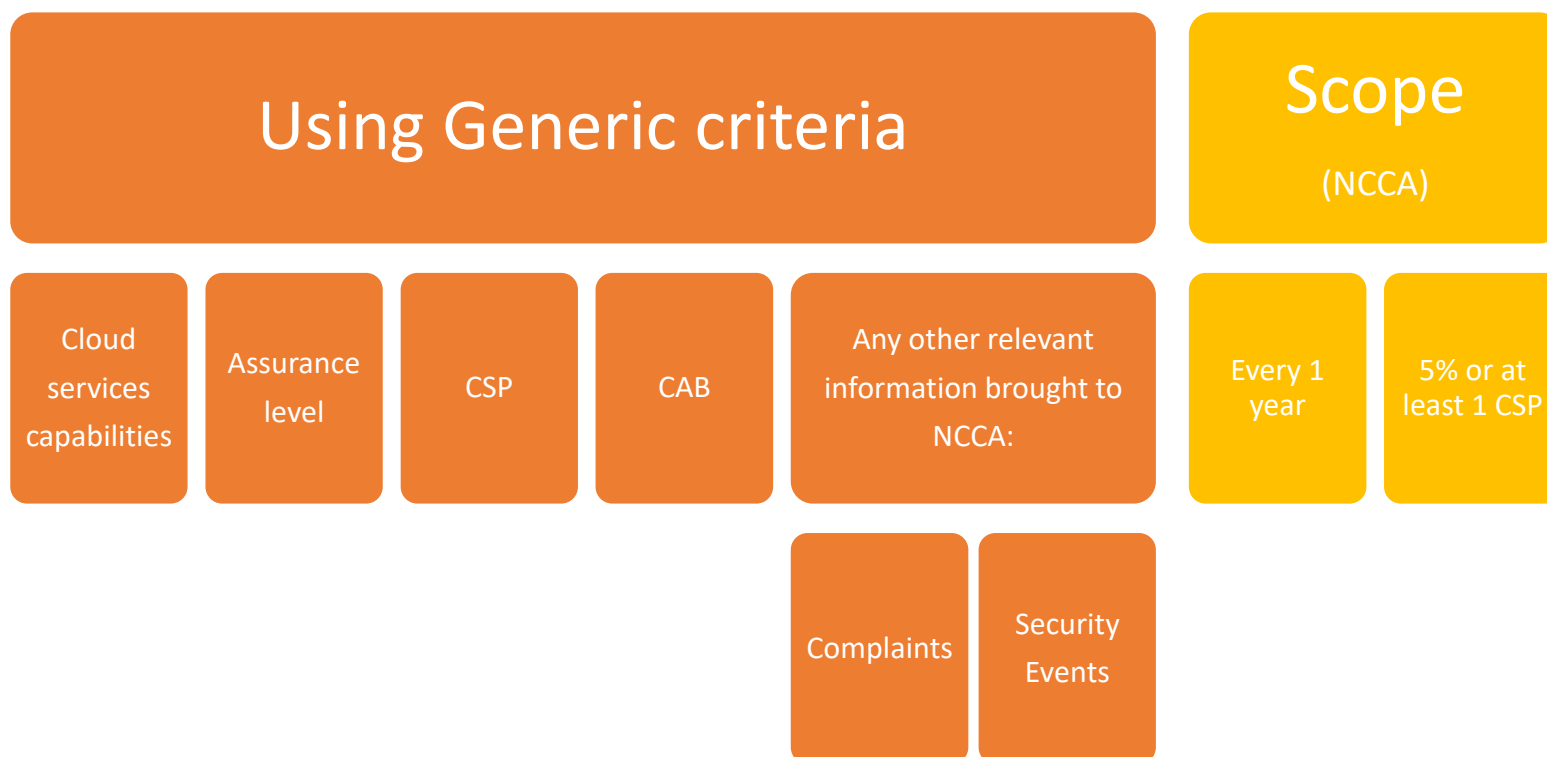
ECCF LOGO*	EUCS LOGO*
Certified in the European Union 	ECCF ENISA website 
CSA – Assurance Level (<i>basic</i> / <i>substantial</i> / <i>high</i>)	EUCS-specific Assurance Level name

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

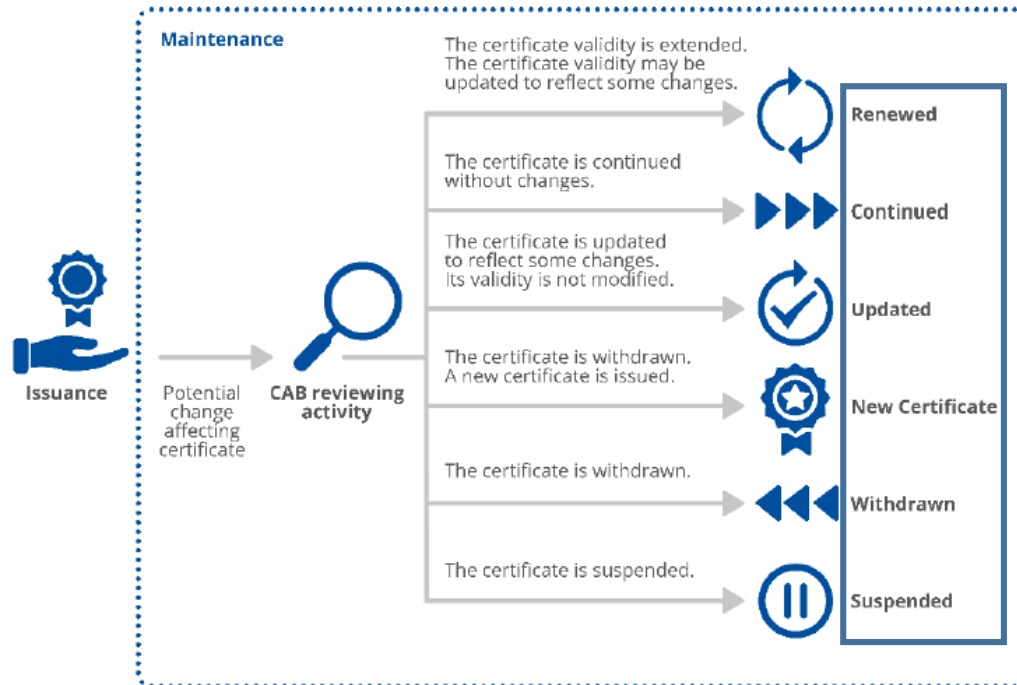
Article 54 (j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

- Cases of non-compliance
 - In the product/service itself
 - Anything that changes the overall security posture
 - New vulnerabilities
 - Data breaches
 - Etc.
 - In respecting certificate usage rules
 - In respecting certificate issuance rules
- Re-assessment of the product/cloud service is more detailed [Annex G](#) (EUCS). Re-assessment either confirms or disproves what is suspected
- Re-assessment are financially supported by the manufacturer/provider

Article 54 (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;



Article 54 (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;



- Maintenance activities can be triggered by:

- Manufacturer/provider
- NCCA
- CAB
- NAB

Article 54 (1) 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;

- Essentially, after a non-compliance is determined, a provider has 14 days for EUCS 'high' level or 30 days for EUCS 'substantial' or 'basic' level to correct it, otherwise first automatic suspensions are triggered, and ultimately these can lead to withdrawals
- Exact procedures depend on the nature of the non-compliance:
 - o Product/service requirements (see image)
 - o Certificate usage/establishment rules, notifications to relevant bodies...



Image from EUCC (p.47)

Article 54 (m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

- Procedure based on ISO/IEC 30111, with additional specificities
 - Preparation
 - Receipt
 - Verification
 - Remediation development
 - Release
 - Post release
- Disclosure is based on ISO/IEC 29147
- The provider has 5 business days to notify the CAB, and in the meantime starts its vulnerability handling process (from Annex A requirements)

Article 54 (n) where applicable, rules concerning the retention of records by conformity assessment bodies;

- Retention of records by CABs :
 - General rules based on ISO/IEC 17065
 - All relevant records, in order to trace certification steps
 - 7 years retention after certificate expiry/withdrawal

Article 54 (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;

Quick review

Article 57 1. [...] national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). [...]

- We have national schemes in the EU for
 - o France
 - o Germany
 - o Netherlands
 - o Spain
 - o Sweden
 - o Norway
 - o Italy

- It might happen that some will be allowed to remain valid 1 year after the implementing act

Article 54 (p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

Article 54 (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;

Article 54 (r) maximum period of validity of European cybersecurity certificates issued under the scheme;

Article 54 (s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;

Chapter 18
of EUCSChapter 19
of EUCSChapter 20
of EUCS

Certificate format

Availability
of
informationCertificate
validity

Certificate disclosure

Nothing yet

Under
constructionBut see Annex F...
There is a
certification report
format7 years after
expiry/withdrawal

3 years

The certificates
shall be disclosed
by ENISA on a
dedicated websiteThey may be
disclosed by NCCAs
and/or related
certification bodies
on their websites

Article 54 (t) conditions for the mutual recognition of certification schemes with third countries;

- The mutual recognition of certification schemes with third countries shall be supported by the establishment of a Mutual Recognition Agreement (MRA) between the participants
- The conditions for recognition of certificates by participants shall include a minimum of conditions :

The participants shall commit themselves to recognise applicable conformant certificates by any accepted Participant

Acceptance of participants shall confirm that the evaluation and certification processes have been carried out in a duly professional manner

ICT security evaluation criteria are to be those laid down in Chapter 8 (Evaluation Methods and Criteria) of EUCS

Others...

Article 54 (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.

Supplementary cybersecurity information defined in Article 55 of the CSA shall be provided during conformity assessment by CSPs to the CAB

Those information shall

URL¹ (link) to the website and relevant pages where information are available

Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the cloud services

Be available in electronic form and in english language.

Remain available at least until the expiration or withdrawal of the corresponding EUCS certificate

Be updated as required to reflect the evolution of the cloud service

¹ The URL (link) to the website shall be part of the certificate

Security Profiles

Principles for **specific requirements**

Shall be
published
on ENISA's
Website

**May be
added to
CSP's
EUCS
certificate**

**Shall not
remove or
weaken
requirement
from EUCS**

Shall specify
EUCS
targeted
**assurance
level**

...

Force majeure cases

Temporary measures by NCCA

NCCA shall
inform
ENISA

ENISA shall
make the
information
available on
their
website

NCCA shall
inform ECCG

ECCG shall
coordinate
with other
NCCA

Extending the
deadlines for
periodic
renewal
assessments

Relaxing
requirements
of conformity
assessment
activities

Extending
validity of
certificate

Protection of information

Professional
secrecy

Intellectual
property

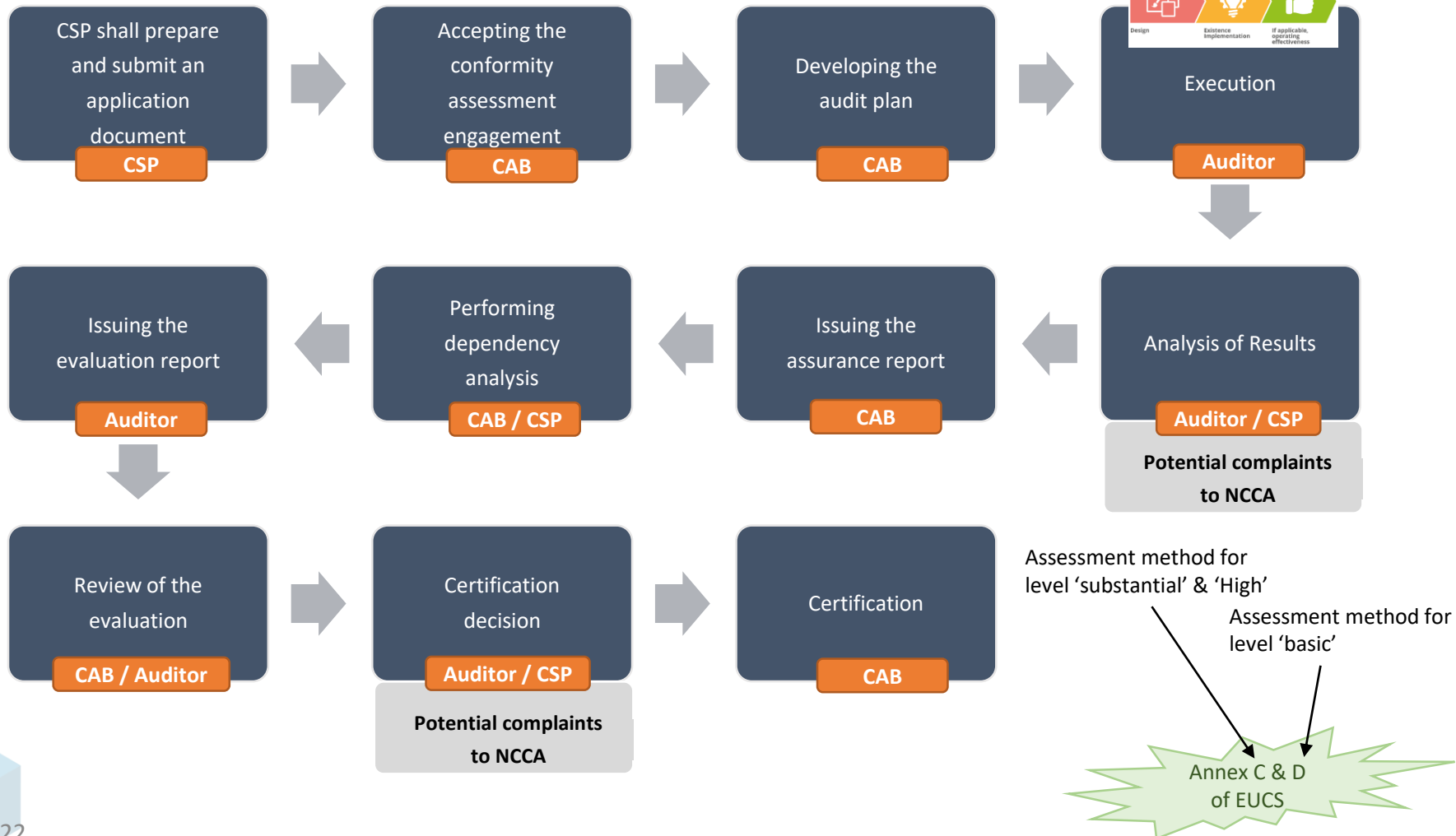
NDA

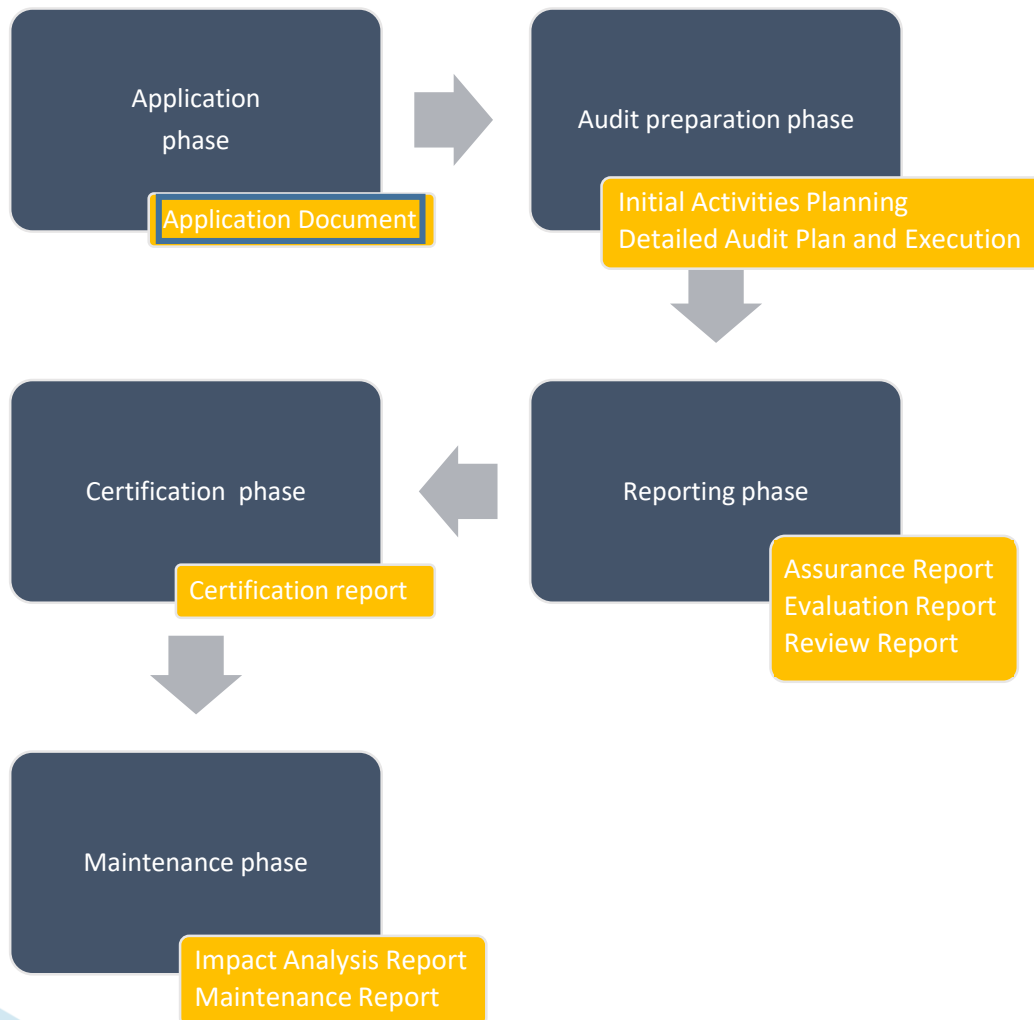
...

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

- A.1 ORGANISATION OF INFORMATION SECURITY
- A.2 INFORMATION SECURITY POLICIES
- **A.3 RISK MANAGEMENT**
- A.4 HUMAN RESOURCES
- A.5 ASSET MANAGEMENT
- A.6 PHYSICAL SECURITY
- A.7 OPERATIONAL SECURITY
- A.8 IDENTITY, AUTHENTICATION, AND ACCESS CONTROL MANAGEMENT
- A.9 CRYPTOGRAPHY AND KEY MANAGEMENT
- A.10 COMMUNICATION SECURITY
- A.11 PORTABILITY AND INTEROPERABILITY
- A.12 CHANGE AND CONFIGURATION MANAGEMENT
- A.13 DEVELOPMENT OF INFORMATION SYSTEMS
- A.14 PROCUREMENT MANAGEMENT
- A.15 INCIDENT MANAGEMENT
- A.16 BUSINESS CONTINUITY
- A.17 COMPLIANCE
- A.18 USER DOCUMENTATION
- A.19 DEALING WITH INVESTIGATION REQUESTS FROM GOVERNMENT AGENCIES
- A.20 PRODUCT SAFETY AND SECURITY (PSS)

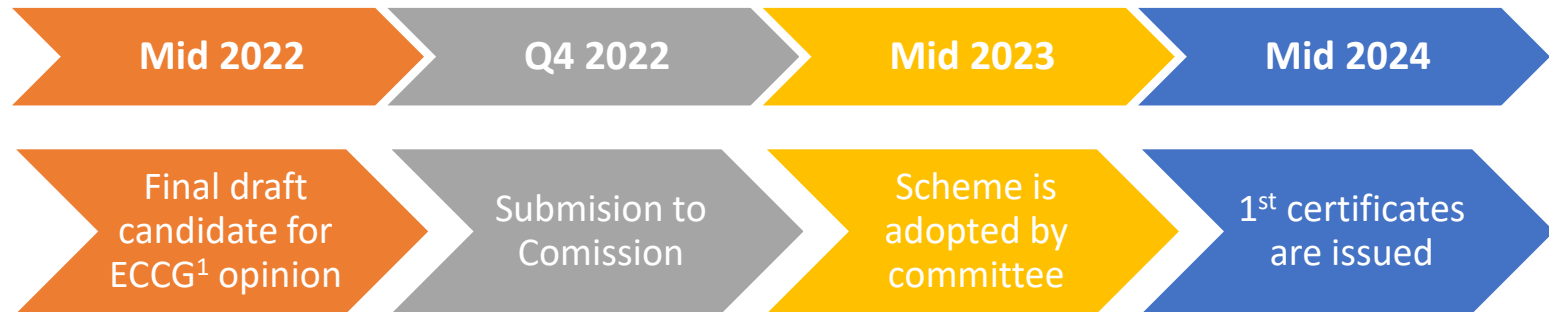
- The structure of this meta approach starts with defining a **clear objective**, followed by the development and execution of an **audit plan**, and ending with the analysis of the gathered evidence and the delivery of an **assurance report**.



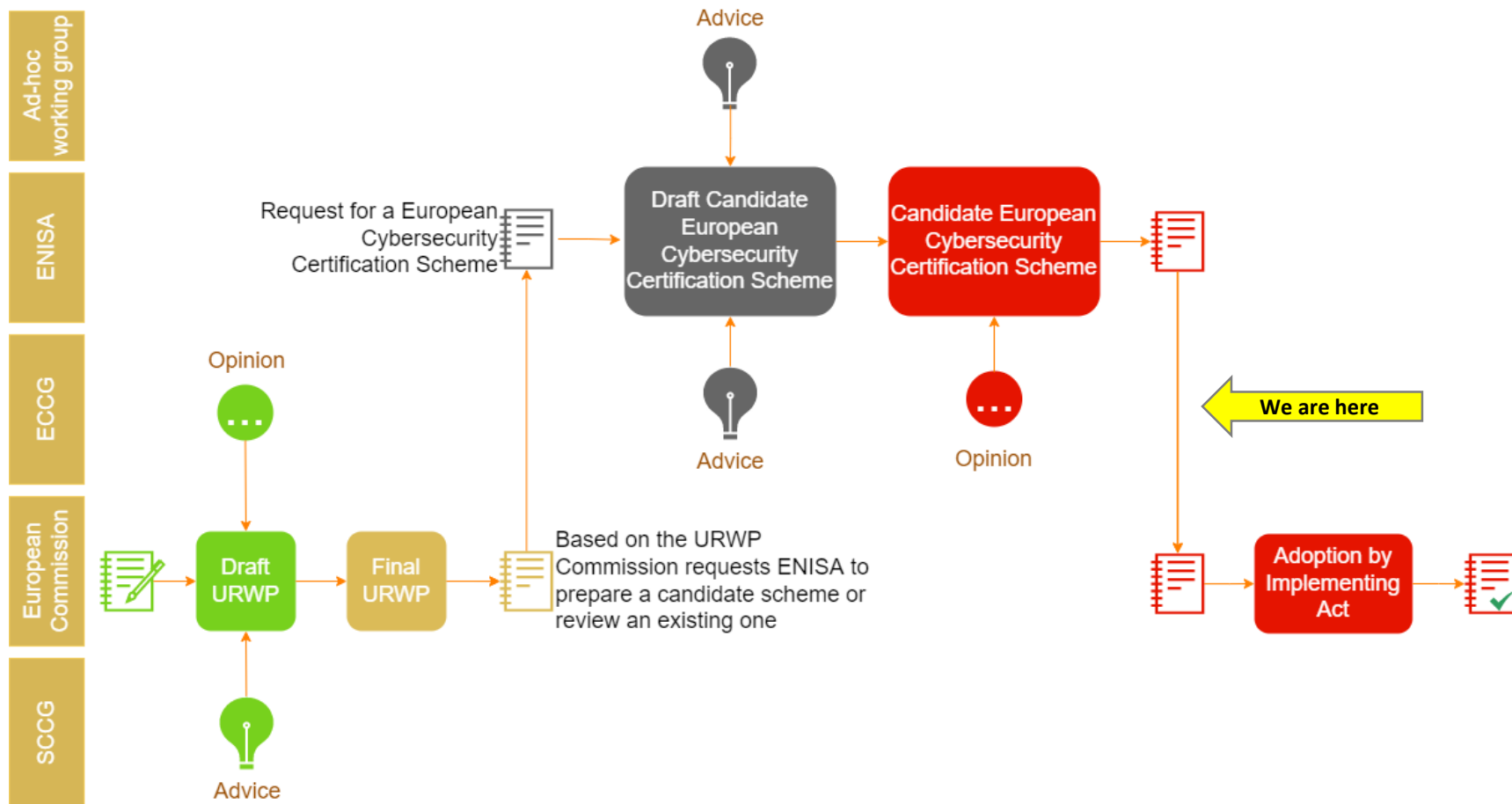


Mandatory field in the template	Clarification
Section 1: "Identification" This section identifies the Cloud Service for which the evaluation application is submitted.	
CSP Identity	Identity of the CSP requesting the evaluation.
CSP Contact	Identification and contact details for the lead contact at the CSP that will support the evaluation process.
Service Name	Commercial name of the CSP Cloud Service for which the evaluation is requested.
Short Description	A short description of the functionality of 'Service Name'.
Assurance Level	The assurance level for which the evaluation is requested. Valid values are 'Basic', 'Substantial', or 'High'.
Security Profiles	The list of security profiles applicable to the cloud service
Application Type	CSP specified evaluation application type. Valid values are 'initial', 'periodic', 'renewal' or 'restoration'.
Application Period	When applicable, the period to be considered by the CAB for the assessment of operational effectiveness.
Section 2: "Claim" This section is the CSP's management assertion the template accurately and fairly describes the Cloud Service and the applicable controls from the scheme's framework.	
Claim	This is a written conformity statement by the management of the CSP.
Section 3: "CSP's Description of its service" This section is the CSP's assessment of the Cloud Service's implementation of the scheme's requirements and control framework.	
3.1: Types of Services	The specific functional purposes of the Cloud Service.
3.2: Service Components	This is a document label for reference purpose, no text required.
- Physical Infrastructure	The physical structures of the service, datacentre, server, other hardware.
- Software	The programs and system software that supports programs, that are part of the service
- People	The personnel involved in the governance, operation and use of a service
- Policies and procedures	The policies and automated and manual procedures involved in the operation of a service
- Data	the information used and supported by a service (transaction streams, files, databases and tables).
3.3: Service Boundaries	The boundaries of the system subject to certification
3.4: Sub Services	The sub-services that are material to the operation of the Cloud Service

- Assessment during maintenance (triggered by **CAB**)
 - conformity assessment may be simplified
 - Periodic assessment
 - Analysis of the change in the cloud service
 - Partial reassessment of controls
 - Effectiveness assessment
 - Renewal assessment
 - Restoration assessment
 - Ad hoc assessment (triggered by **CSP**)
- Re-assessment and audits for compliance monitoring (triggered by the **NCCA**)
 - Re-assessment
 - Compliance audits



¹ European Cybersecurity Certification Group (members: EC, Enisa, CB, EU members)





Thank you
Merci
Danke

ILNAS

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux

Tel. : (+352) 24 77 43 - 01 · Fax : (+352) 24 79 43 - 10

E-mail : info@ilnas.etat.lu

www.portail-qualite.lu