RED ALERT LABS
IoT Security

TrustBoost Training - Day 2

European Union Cloud Services Scheme (EUCS)

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

29/10/2024

TrustBoost

Agenda

"The secret to getting ahead is getting started."

TWAIN

1 | Cloud Security Introduction

2 | Introduction to EUCS Scheme

3 | Deep-dive into EUCS

RED ALERT LABS
IoT Security

SECTION 1: INTRODUCTION TO CLOUD SECURITY

Cloud Security introduction

- Cloud Services Definition
- Typical Infrastructure
- Cloud Services examples

Sub-Section 1

Definition

Cloud Services Definition

ISO/IEC 22123-1:2023

Information Technology of **Cloud computing** - PART 1 : **Vocabulary**

ISO/IEC 17789:2014

Define the **reference functional architecture**, i.e. how to build a cloud computing services platform, for the sake of **interoperability**

ISO/IEC 27018:2014

Sets the **security rules** to be applied for public cloud providers in order to **ensure the protection of personal data**, guarantee **transparency** and comply with their **regulatory obligations**.

RED ALERT LABS
IoT Security

ISO/IEC 22123-1:2023

Cloud Services Definition

- ## Cloud Computing

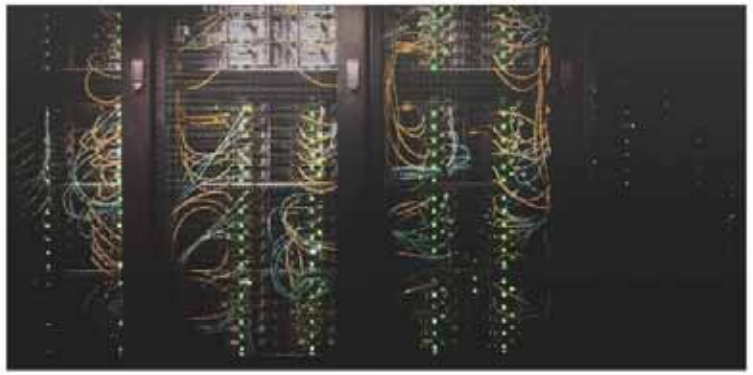
  Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

- ## Cloud Services

  One or more capabilities offered via cloud computing invoked using a defined interface.

- ## Cloud capabilities

  Type in which classification of the functionality provided by a cloud service to the cloud customer can use the cloud services provider's solution



RED ALERT LABS
IoT Security

ENISA

Cloud Services Definition

3 Categories of service models / Cloud capabilities

- **Infrastructure as a Service**

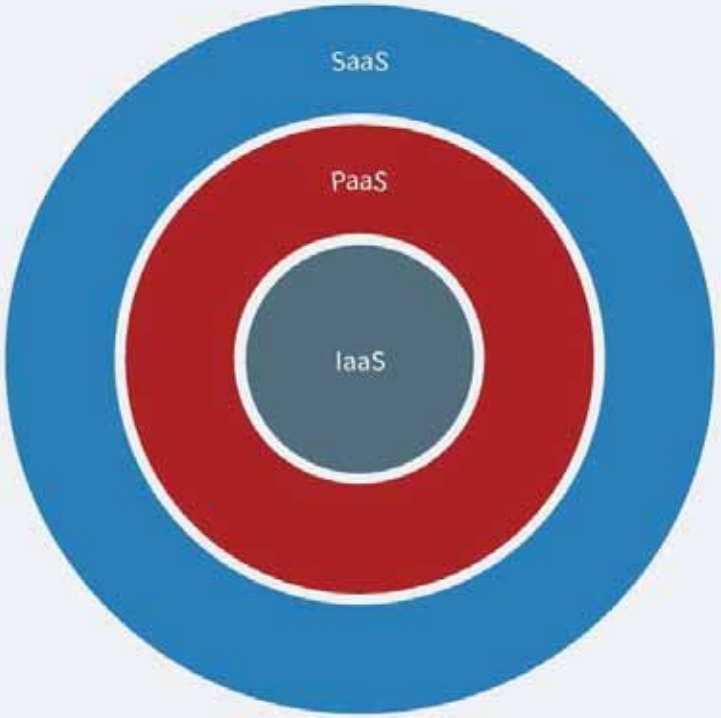
provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API.

- **Platform as a Service**

Allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms.

- **Software as a Service**

Software offered by a third party provider, available on demand, usually via the Internet configurable remotely.



RED ALERT LABS
IoT Security

ENISA

Cloud Services Definition

Deployement models

Public

Available publicly.

Any organisation may subscribe

Private

Services built according to cloud computing principle but accessible only within a private network

Partner or Community

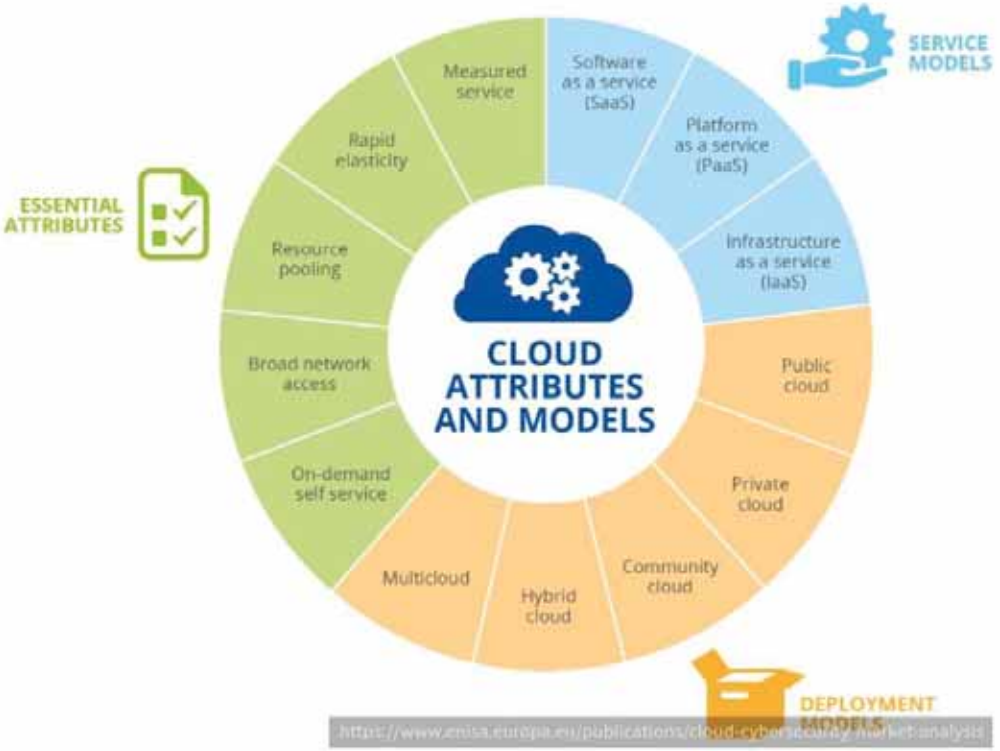
Cloud services offered by a provider to a limited and well definde number of parties

RED ALERT LABS
IoT Security

ENISA

Cloud Services Definition

Summary



RED ALERT LABS
IoT Security

ENISA

Cloud Services Definition

EUCS - ICT Services coverage criteria - What is a "cloud services"?

Criteria #1

The ICT service implements one or more capabilities offered via cloud computing invoked using a defined interface [ISO22123].

Criteria #2

The ICT service aims at reaching the assurance level corresponding to one of the three levels ‘basic’, ‘substantial’ and ‘high’ of the EUCSA as defined in the EUCS scheme

RED ALERT LABS
IoT Security

Sub-Section 2

Infrastructure

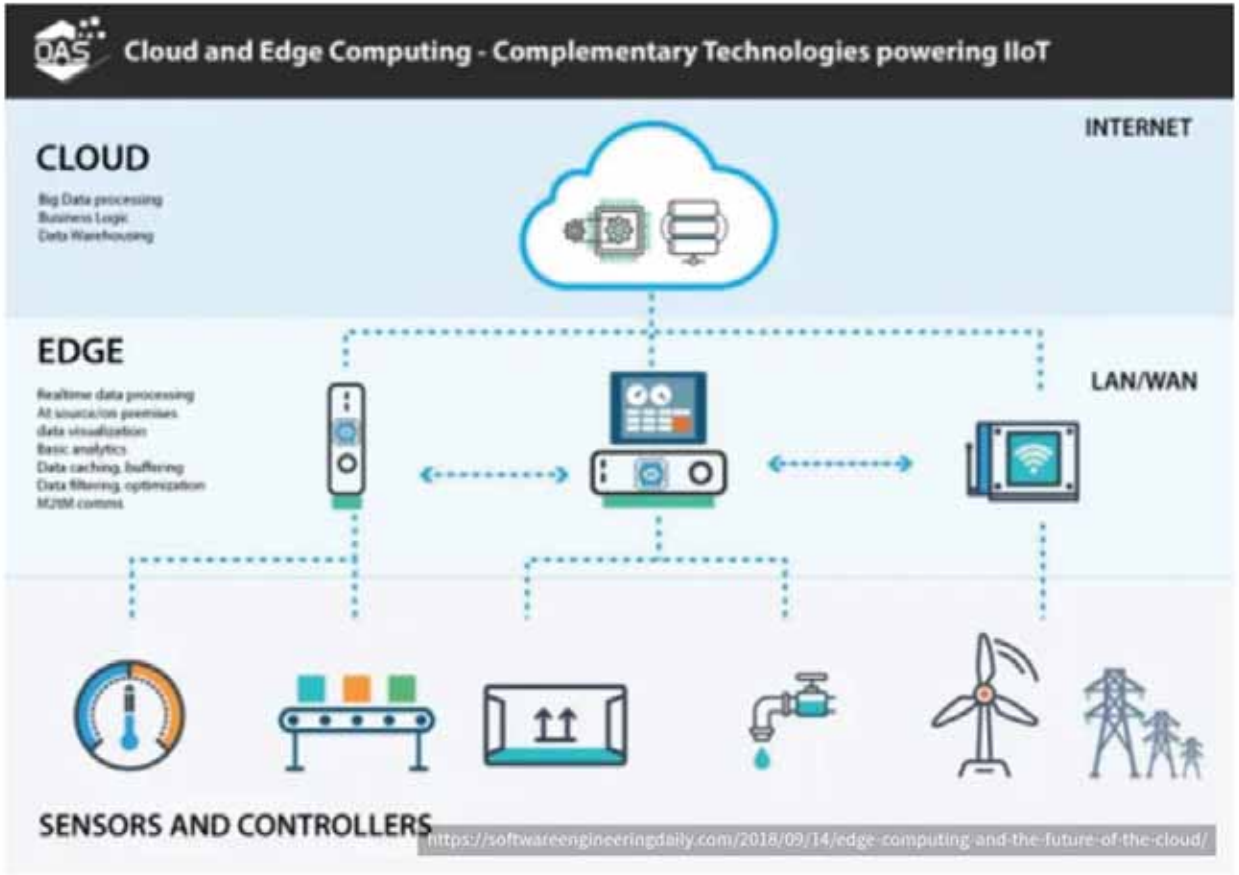
Typical Cloud infrastructure

Different abstraction layers

RED ALERT LABS
IoT Security

Typical Cloud infrastructure

Edge computing parenthesis



RED ALERT LABS
IoT Security

$1 T

THE VALUE OF THE CLOUD COMPUTING MARKET WILL REACH $1 TRILLON IN 2028

635%

JUMP BETWEEN 2010 AND 2020

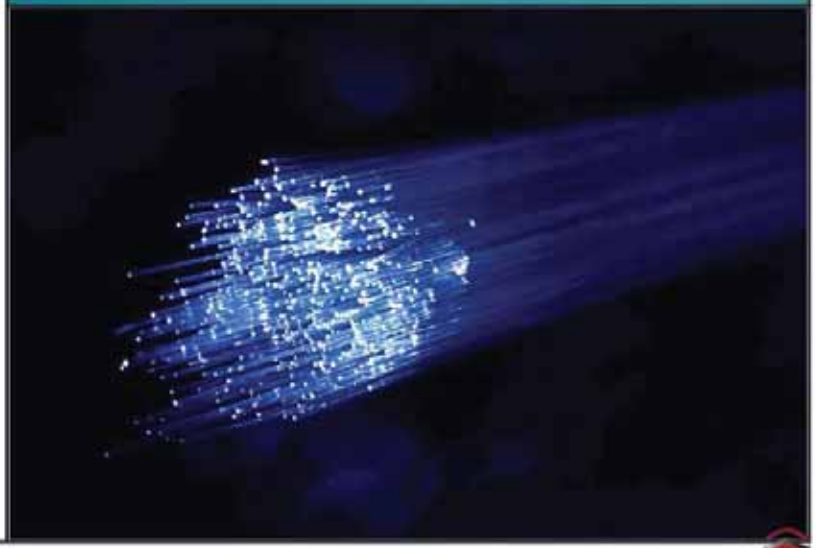
200 ZB

BY 2025, TOTAL CLOUD STORAGE EXPECTED TO REACH 200 ZETTABYTES.

(1 ZB = 10^21 B ≈ 1,000,000,000 TB).

CLOUD USAGE

9/10 Compagny



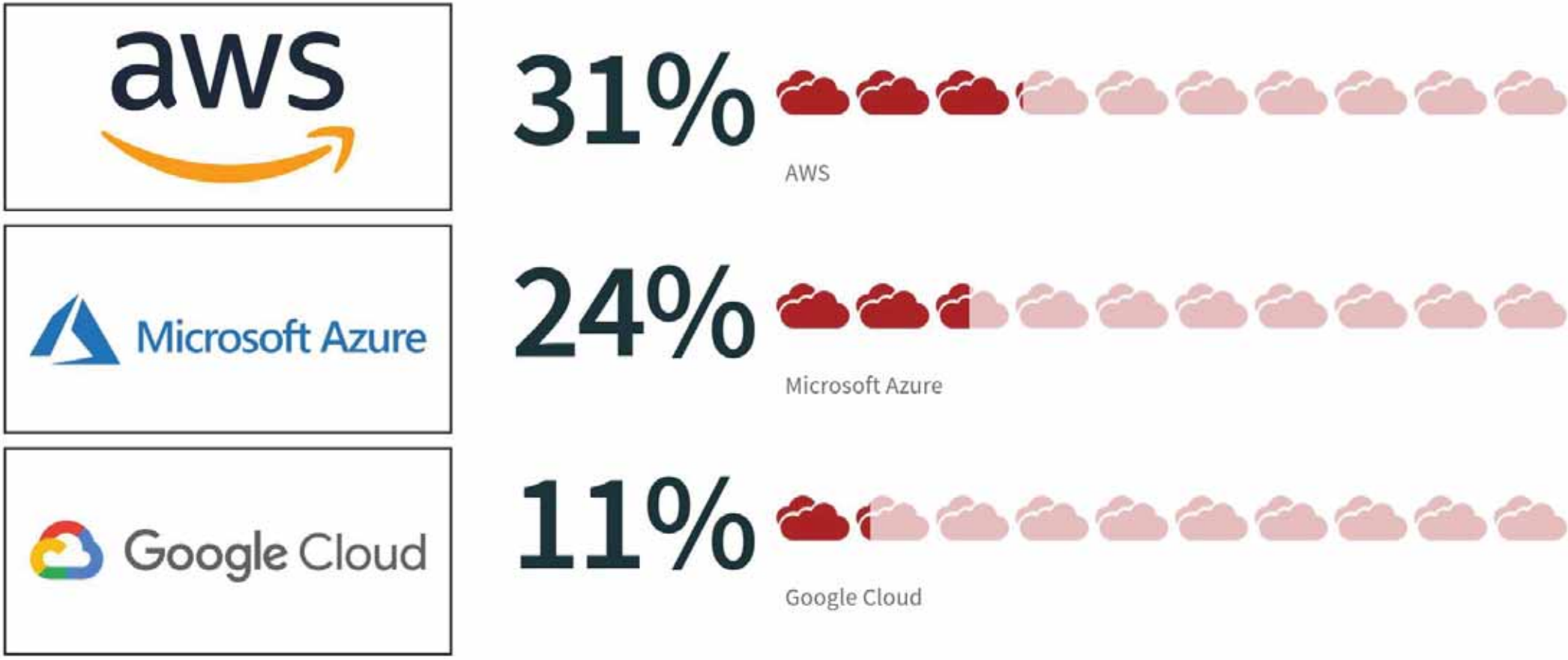
RED ALERT LABS
IoT Security

Cloud Services Examples

RED ALERT LABS
IoT Security

Cloud

Market Share



Cloud

Domains

In this **highly digitalized era**, cloud computing offers **immense benefits** to a wide range of industries. It **reduces storage costs** while at the same time **increasing storage capacity**, and it is **flexible** enough to **adapt to any business environment**.

RED ALERT LABS
IoT Security

Question time

- ✔ Question #1
  Could you name the 3 Cloud services models / Cloud capabilities ?
- ✔ Question #2
  What makes these cloud service models different?
- ✔ Question #3
  What are the advantages to use a private cloud ?
- ✔ Question #4
  What are the criterias to be in the scope of the EUCS ?

RED ALERT LABS
IoT Security

Answer

- ✔ Could you name the 3 Cloud services models / Cloud capabilities ?

  -Iaas, PaaS, SaaS,

- ✔ What makes these cloud service models different?

  - the level of abstraction and management they offer to users,

  - the sharing responsibilities between CSP and cloud services users

- ✔ What are the advantages to use a private cloud ?

  - offer greater control and customization over security policies and configurations

  - can be customized to meet the specific needs and requirements of an organization

- ✔ What are the criterias to be in the scope of the EUCS ?

  - The service implements one or more capabilities offered via cloud computing using a defined interface

  - The service aims at reaching the assurance level corresponding to one of the three levels 'basic', 'substantial' and 'high' of the EUCSA as defined in the EUCS scheme

RED ALERT LABS
IoT Security

Sub-Section 3

What about security

Risk Analysis

The cloud Attack Surface

External Threats

- Malware
- Zero-days
- Account Takeovers

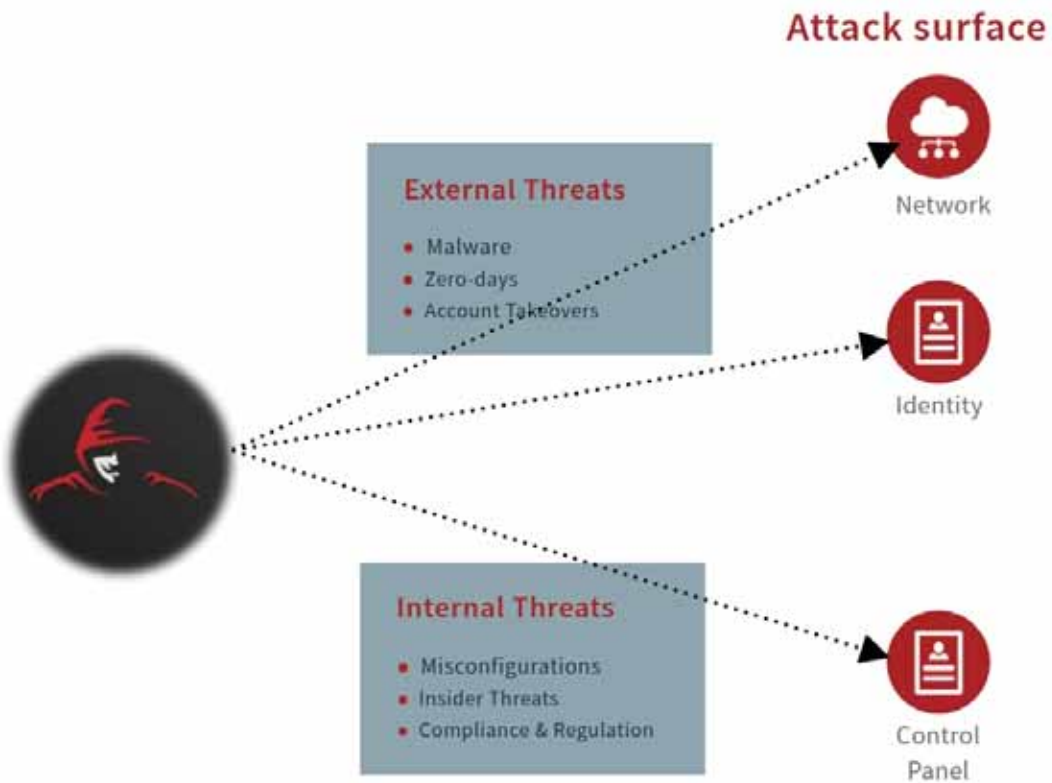
Internal Threats

- Misconfigurations
- Insider Threats
- Compliance & Regulation

RED ALERT LABS
IoT Security

Risk Analysis

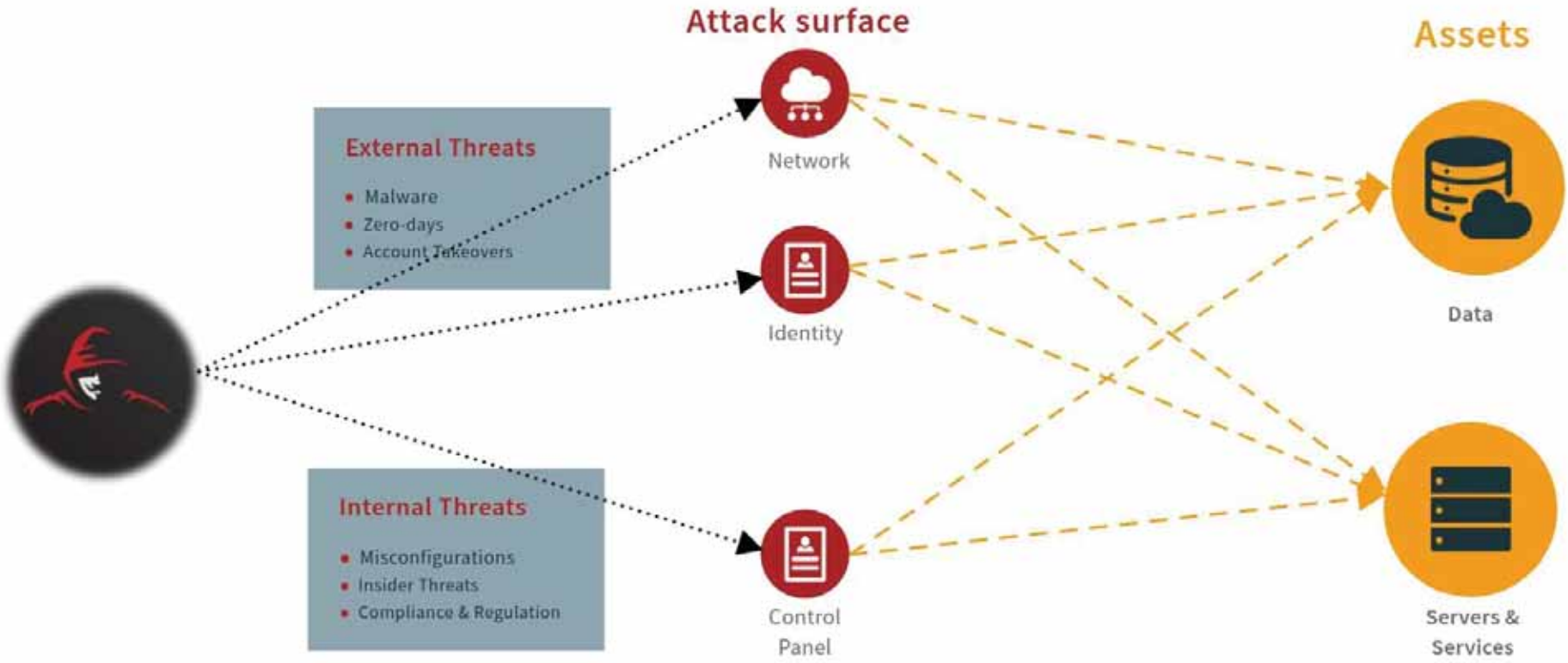
The cloud Attack Surface



RED ALERT LABS
IoT Security

Risk Analysis

The cloud Attack Surface



RED ALERT LABS
IoT Security

Risk Analysis

Example of assets

From ENISA

Company Reputation

Personal Data

Network Connexion

Customer Trust

Services Delivery

Physical Hardware

Intellectual Property

Access Control

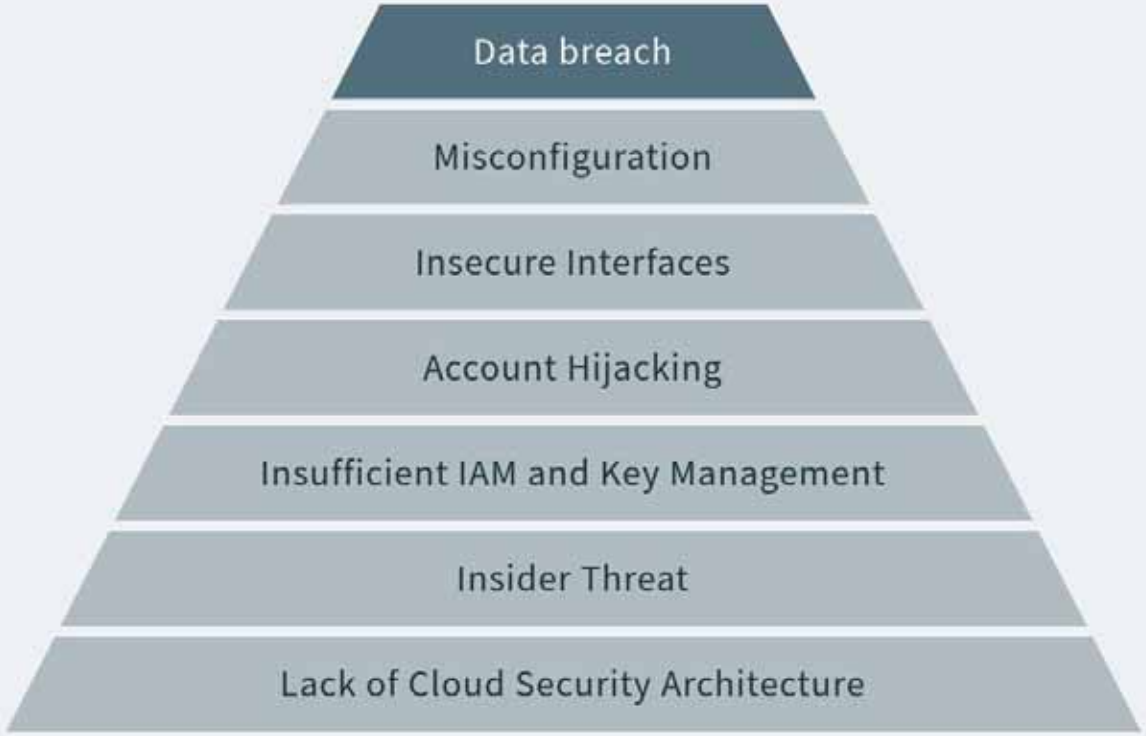
Backup or Archived Data

RED ALERT LABS
IoT Security

Risk analysis

Major threat

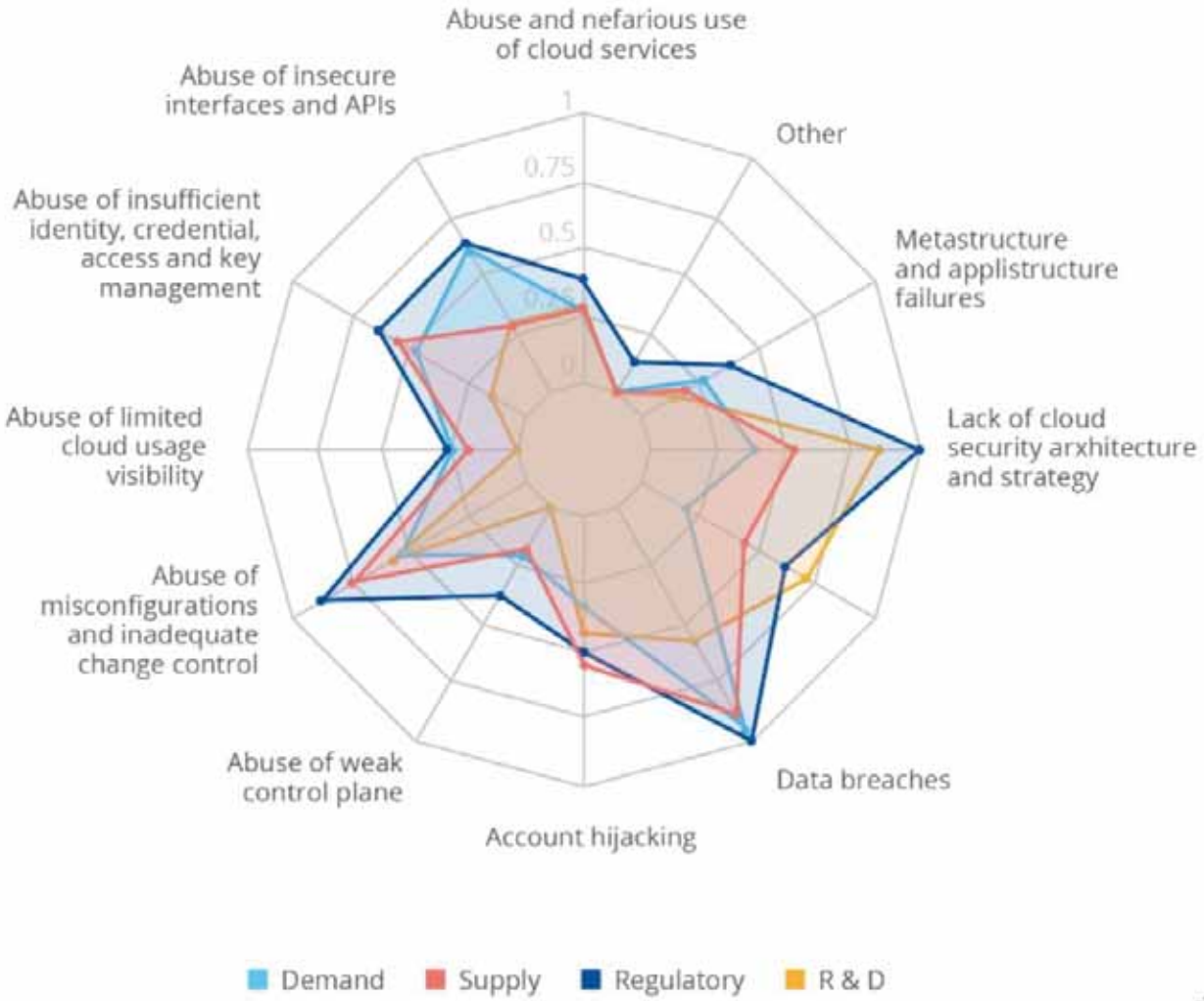
From Cloud security Alliance / ENISA



Risk analysis

Major threat

From Cloud security Alliance / ENISA



RED ALERT LABS
IoT Security

Risk analysis

Major Challenges for Cloud Security

From ENISA

Acces Control / Authorisation

Chain of Trust

Storage / Network Security

Identification and Authentication

Compliance

Confidentiality, Availability, Integrity

Audit

Cybersecurity Incident Management

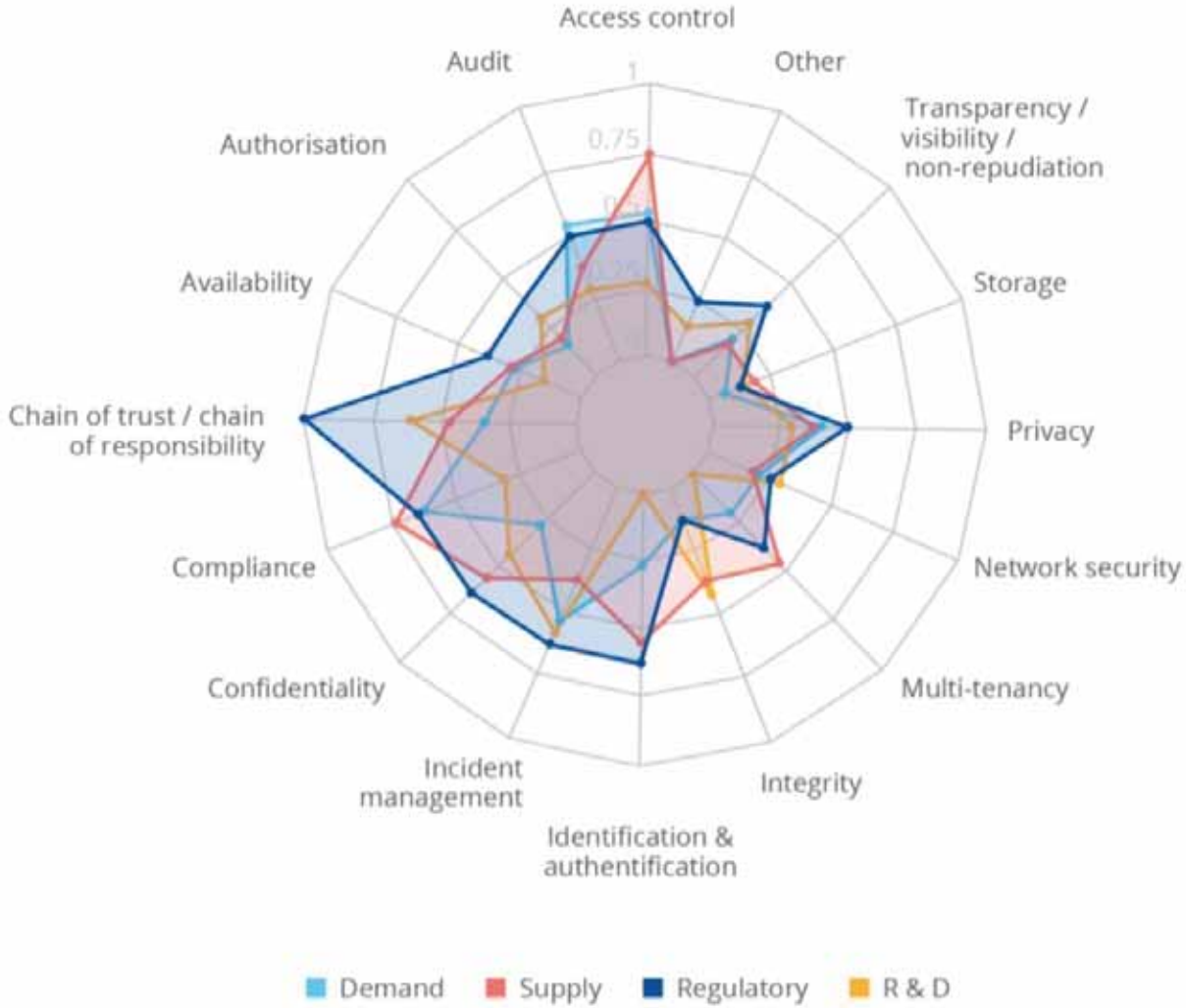
Privacy

RED ALERT LABS
IoT Security

Risk analysis

Major threat

From Cloud security Alliance / ENISA



RED ALERT LABS
IoT Security

Question time

- **Question #1**
  Could you name 2 sensitive assets of the Cloud Infrastructure?
- **Question #2**
  Could you name 1 major threat that is targeting cloud ?
- **Question #3**
  Could you name 2 challenges for Cloud security?

RED ALERT LABS
IoT Security

Answer

- Could you name 2 sensitive assets of the Cloud Infrastructure?

  -Could you name 2 sensitive assets of the Cloud Infrastructure?

- Could you name 1 major threat that targeting cloud ?

  Data breach, misconfiguration, ...

- Could you name 2 challenges for Cloud security?

  - Access controls, audit, chain of trust, network security

RED ALERT LABS
IoT Security

A

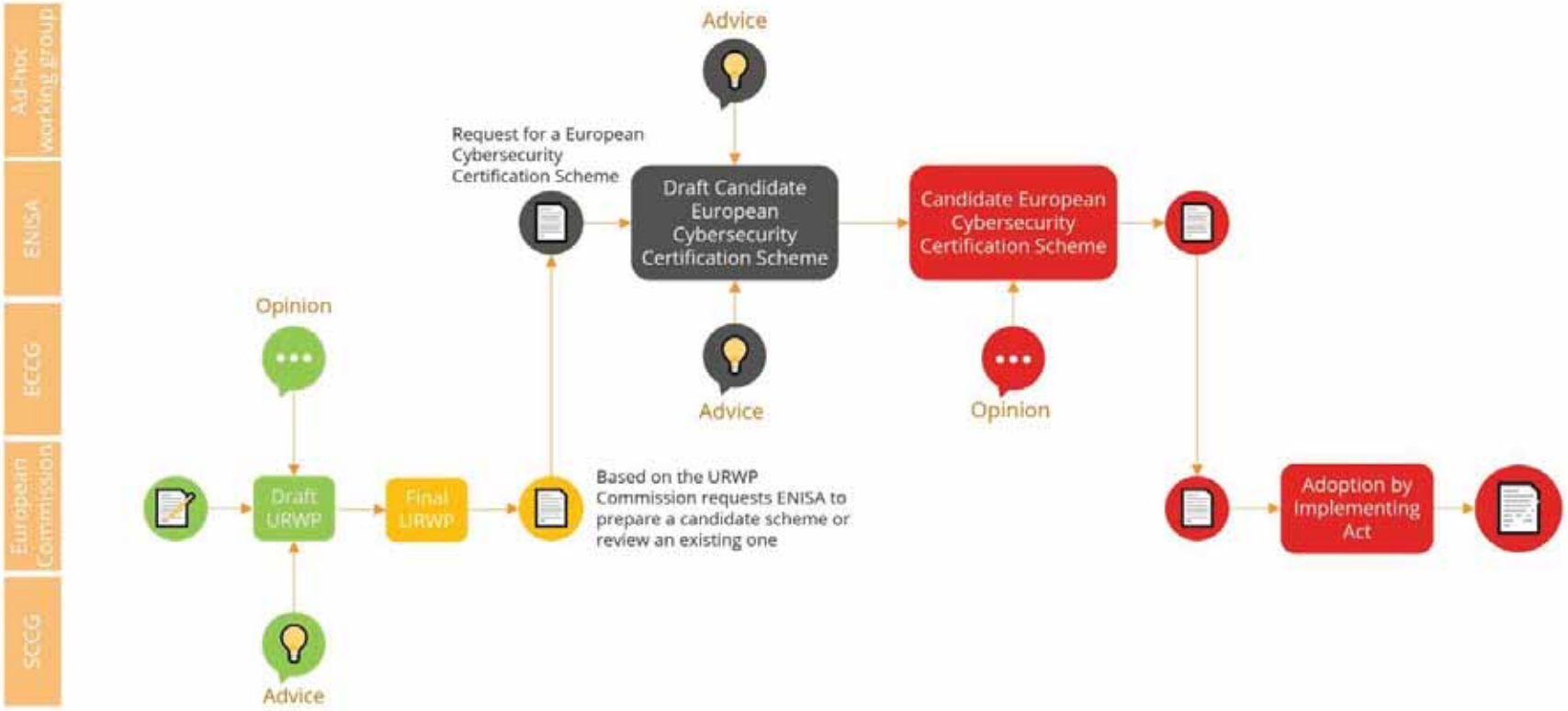
SECTION 2:

EUCS introduction

EUCS introduction

Stakeholders

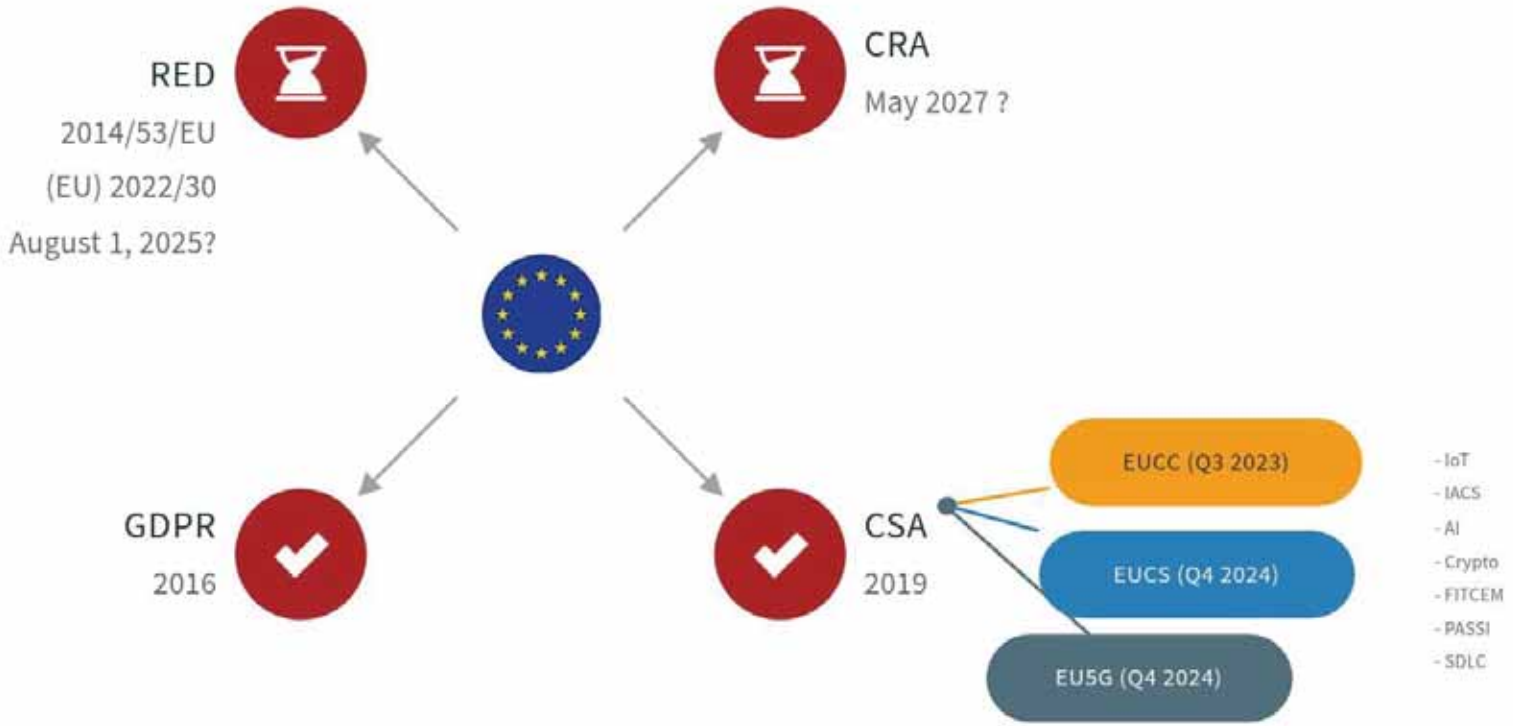
Adoption process



RED ALERT LABS
IoT Security

Regulation

Europe



RED ALERT LABS
IoT Security

Schemes related to Cybersecurity Act

EUCC

COMMON CRITERIA BASED EUROPEAN CANDIDATE CYBERSECURITY CERTIFICATION SCHEME

Objective : certification of cybersecurity of ICT products, based on the Common Criteria, the Common Methodology for the evaluation of information technology security (CEM) and the corresponding standards, respectively ISO/IEC 15408 and ISO/IEC 18045 .

EUCS

EUROPEAN CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES

Objective : cloud services cybersecurity certification

5G

Under development

EUDIW

To come

IoT

To come or not!

The EU Certification Scheme for Cloud Services

An overview

- **Aims**
  - Establishing the conformity of cloud services to a set of requirements corresponding to one of the evaluation levels defined in the EUCS;
  - Providing sufficient information to prospects and customers with adequate cybersecurity knowledge for making informed security decisions on cloud services, allowing them to fully understand and implement the documentation that defines their responsibility.
- **Universal**

  Does not distinguish between different categories of cloud services, unless explicitly stated in a specific rule or requirement.

  Covering the 3 main cloud service models (IaaS / PaaS / SaaS)
- **Focus on Cybersecurity**

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

  The three assurance levels of the CSA are taken into account in EU Certification Scheme for Cloud Services.

  Basic (mandatory certification) / Substantial / High
- **Responsibility sharing**

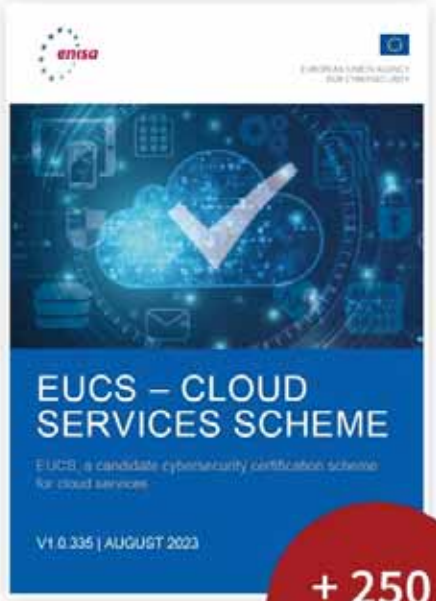
  EUCS acknowledges that the responsibility for the security of a cloud service is split between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC), and aims at verifying that this split of responsibility is explicitly and publicly documented by the CSP;
- **Challenges:**

  Ensure that EUCS High takes over the requirements of SecNumCloud, while keeping compliance with the C5 German scheme

RED ALERT LABS
IoT Security

Some definitions

Reuse from ISO/IEC 22123-1



+ 250
DEFINITIONS

1 | **Cloud Service Customer**
CSC
Party which is in a business relationship for the purpose of using cloud services

2 | **Cloud Service user**
CSU
Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services

3 | **Cloud Service Provider**
CSP
Party which makes cloud services available

4 | **Primary CSP**
In inter-cloud computing, a cloud service provider which is making use of cloud services of secondary cloud service providers as part of its own cloud services

5 | **Secondary CSP**
Cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services

6 | **Cloud Capabilities type**
Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used

7 | **CSC data**
Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service

8 | **CSP data**
Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider

9 | **Cloud Service Extension profile**
CSEP
A document defining extended requirements to complement the EUCS in a specific context

RED ALERT LABS
IoT Security

EUCS Introduction

Generic information about the scheme

CABs

Based on the ISO/IEC 17065 standard in terms of applicable requirements to CABs performing certification

Not Standalone

The EUCS scheme is not a standalone scheme; it is part of the European cybersecurity certification framework.

Draws significantly

From the German C5 Scheme

Insipiration from

- the French SecNumCloud
- the proposals in the SCP-CERT report
- the principles in other schemes used in Europe

'Basic' simplified Methodology

- simplified assessment methodology for the EUCSA assurance level 'basic'.
- based on a self-assessment performed by the CSP
- Result reviewed by the CAB

RED ALERT LABS
IoT Security

EUCS road to EC Adoption: A Tentative Timeline

RED ALERT LABS
IoT Security

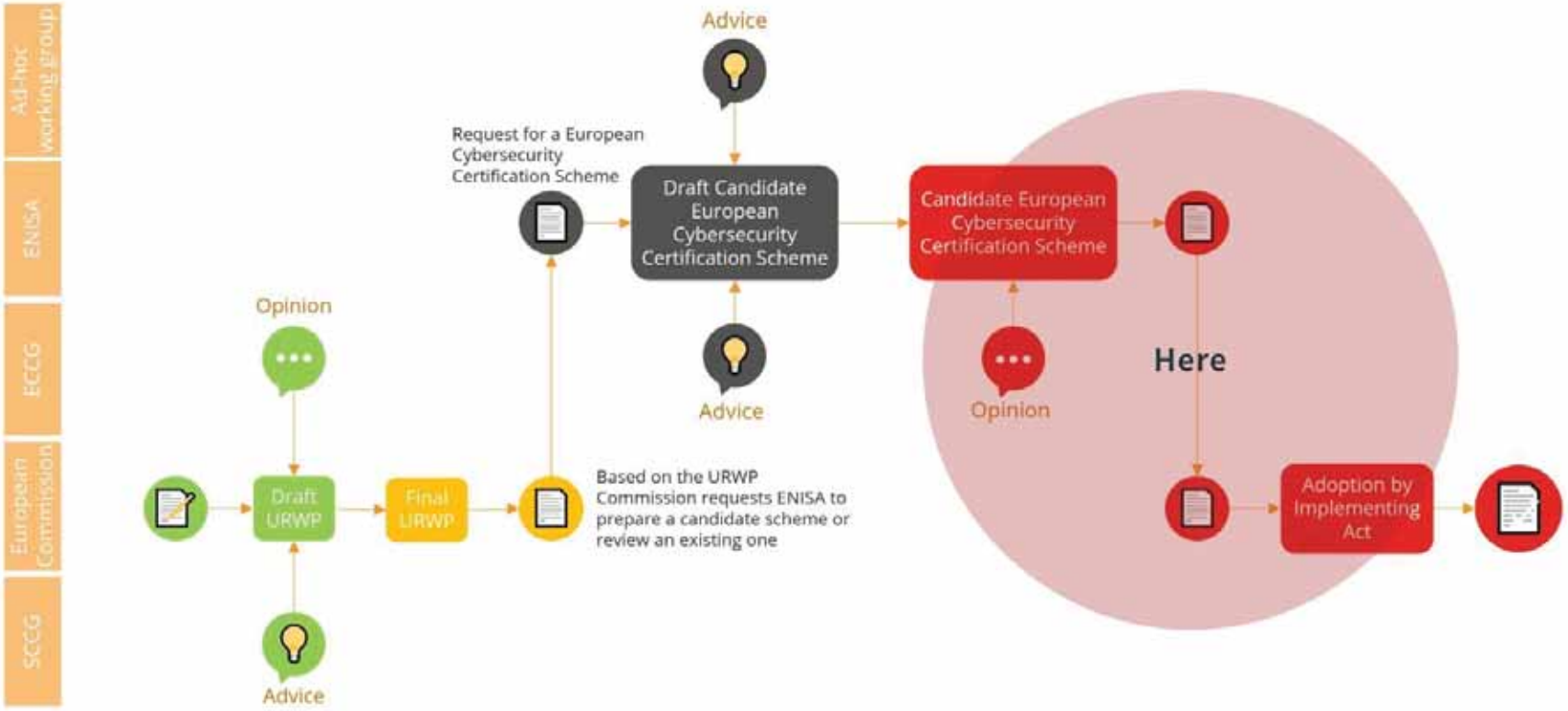
EUCS road to EC Adoption: A Tentative Timeline

RED ALERT LABS
IoT Security

EUCS introduction

Stakeholders

Adoption process



RED ALERT LABS
IoT Security

EUCS - introduction

Relation with other schemes

This scheme will be a regulation, similar to National schemes

- If national schemes in europe are deemed equivalent, then they shall stop emitting certificates and be replaced by the european scheme
- In that case, a transition will be organized between the scheme, in particular regarding the recognition of certificates and of objective evidence obtained previously
- There may be official mutual recognition with third countries, but none is foreseen at this stage

There is no formal relationship with private schemes

- There will be neither transition nor recognition
- We are aware that these schemes will co-exist
- A key objective is to enable optimized certification strategies, with significant reuse of objective evidence

RED ALERT LABS
IoT Security

EUCS introduction

Where can I find the latest version ?

EUCS – Cloud Services Scheme

This publication is a draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services), which looks into the certification of the cybersecurity of cloud services. In accordance with Article 48.2 of the Cybersecurity Act1 (EUCSA), ENISA has set up an Ad Hoc Working Group (AHWG) to work on the preparation of the candidate scheme on cloud services, as part of the European Cybersecurity Certification Framework. This is a draft version to be used as basis for an external review. The objective of the review is to validate the principles and general organization of the proposed scheme, and to gather feedback on the proposed wording of the sections and annexes.

Download
PDF document, 3.31 MB

Published December 22, 2020
Language English

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

Upcoming publications

- TS 18026 - "Management systems and controls sets"
  Requirements for cybersecurity of cloud services.
- TS 18072 "Security evaluation and assessment"
  Requirements for conformity assessment bodies certifying cloud services
- New Version of the EUCS
- Implementing Act
- Other guidance (e.g. guidance on requirements)

RED ALERT LABS
IoT Security

EUCS introduction

Structure of the Scheme

EUCSA Art 54.1

Chapter 2 to 23 follow the same structure. Each one of them provides content related to one othe points raised in Article 54(1). There are 22 such points, number (a) to (v). So there is 22 chapters this, chapter from 2 to 23.

Every chapter contains the following sections:

- An extract from Article 54(1) defining the topic addressed in the chapter
- Content defining scheme rules and requirements. Use of "shall" to express a requirement and "may" for an option
- A rationale providing additional information, reasons for making the choices in the proposed text

Additional chapters

1 - A scheme for Cloud Services (introduction)

24 - Additional topics

25 - Further recommendations

26 - References

RED ALERT LABS
IoT Security

EUCS Introduction

Structure of the Scheme

Annexes

Annex A

Security Objectives and requirements for Cloud Service

Annex B

Approach for the assessment of Cloud Service

Annex C

Competence requirements for CABS

Annex D

Scheme document content requirements

Annex E

Certification life cycle and continued assurance

Annex F

Composition

Annex G

Extension profiles

Annex H

Peer assessment

Annex I

Terminology

RED ALERT LABS
IoT Security

EUCS introduction

Structure of the Scheme

EUCSA Art 54.1 - EUCS Chapters 2 to 23

a. Subject matter and scope

b. 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

c. References to the international, European or national standards applied in the evaluation, and if not available to technical specifications

d. One or more assurance levels

e. An indication whether conformity self-assessment is authorized

f. Specific requirements for the CABs

g. Specific evaluation criteria and methods to be used

h. The information necessary for the evaluation or otherwise to be made available by the applicant

i. If applicable, conditions of use of marks and labels

j. Rules for monitoring compliance of certified and self-assessed products

k. Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope

l. Rules concerning the consequences for products that have been certified or self-assessed and do not comply

m. Rules concerning how previously undetected vulnerabilities should be reported and handled

n. Rules concerning the retention of records by CABs

o. Identification of national and international schemes with the same scope

p. Content and format of the certificates and EU statements of conformity

q. The period of the availability of EU statements of conformity and related documentation

r. Maximum period of validity of certificates

s. Disclosure policy for certificate issuance, withdrawal, amendment

t. Conditions for mutual recognition with third countries

u. Where applicable, rules for peer assessment

v. Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

RED ALERT LABS
IoT Security

SECTION 3:

EUCS

Chapter 3

Purpose of the scheme

Chapter 3 - Purpose of the scheme

Why a certification scheme is important?

Certification ➡ Trust

> "TRUST should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes ..."
>
> Cybersecurity Act – Section (7)

> "An increase in trust can be facilitated by Union-wide CERTIFICATION providing for common cybersecurity requirements and evaluation criteria across national markets and sectors."
>
> Cybersecurity Act – Section (7)

RED ALERT LABS
IoT Security

Chapter 3 - Purpose of the scheme

Why a certification scheme is important?

Fragmentation of the cloud computing industry

Same solution ➡ several certification

Currently, cloud computing products and services in France and Germany have to obtain two specific certifications to be accepted across the entirety of the EU:

The secnumcloud and the compliance controls catalogue (C5).

This is a problem because these two certification processes seem to be at odds with each other.

Unify

This will reduce the fragmentation of the cloud computing industry and unify certification.

All EU Member States would accept this single certification and would greatly aid the cloud computing market as it stands today.

RED ALERT LABS
IoT Security

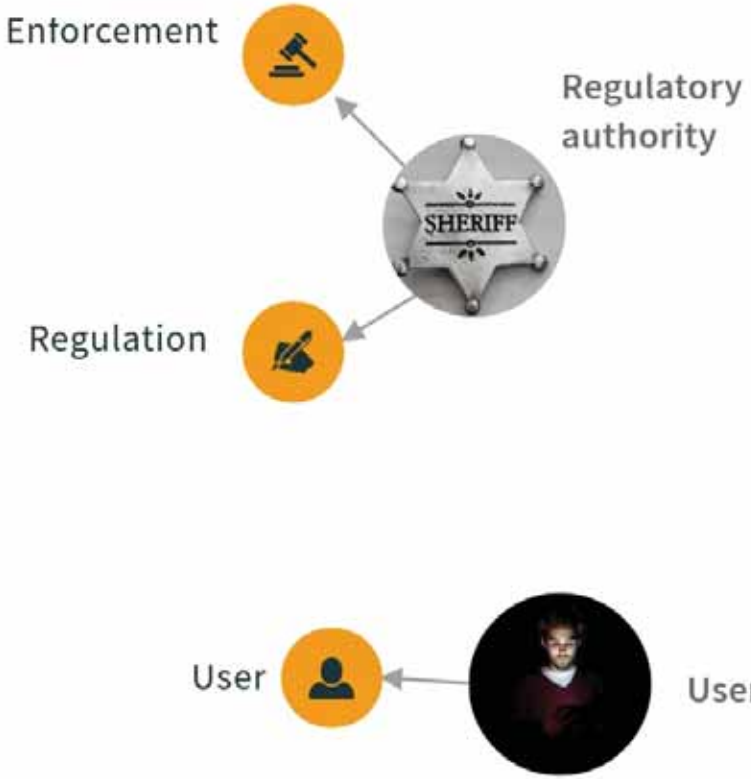
Stakeholder

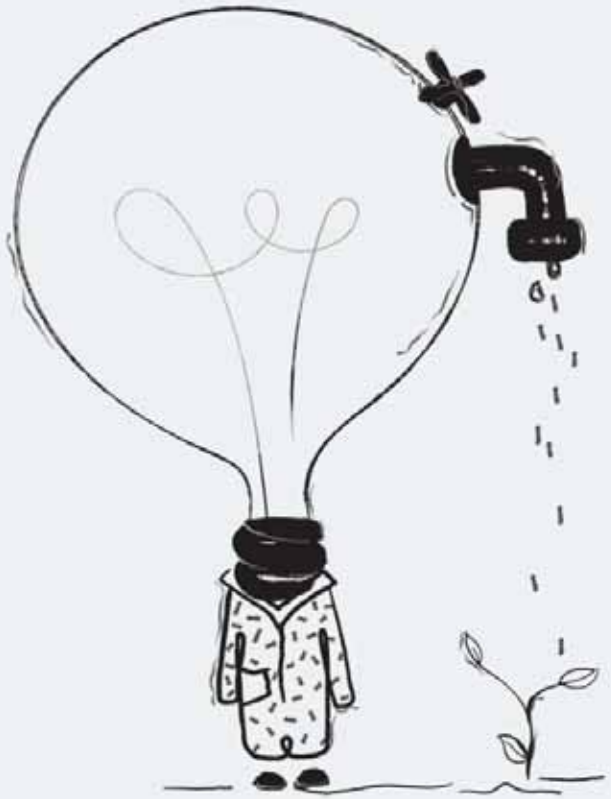
Involves in the production of certificate

Chapter 3 - Purpose of the scheme

Stakeholder

Consuming certificate





The perfect solution ?

Despite these benefits, the **EUCS cannot replace all other mechanisms to get assurance** about the security of a cloud service, at least for the following reasons:

- the responsibility of the security of a cloud service is shared between the CSP, who implement and operate the service, and the CSC, who configure and use the cloud service, and the EUCS only covers the CSP;

- the requirements are defined in three horizontal baselines, mapped to the EUCSA's assurance levels, which represent a consensus between stakeholders about the proper design of controls for cloud services, but they cannot capture the specific requirements of every CSC use case, so it is expected that CSCs and other scheme users define additional cybersecurity requirements to complement those defined in the EUCS as required to cover the risks specific to their use case;

- for some topics where different requirements have been identified for different use cases, the EUCS requires transparency about their controls from CSPs, and the information provided is validated and verified in the evaluation, allowing CSCs to use it in making decisions on security, but in many cases, a CSC's risk assessment will identify some risks that are not covered by transparency requirements;

- the EUCS offers the possibility to define extension profiles when additional requirements are commonly needed in a given context, for instance to satisfy the needs of a category of CSCs or to demonstrate compliance to the cybersecurity requirements of a specific regulation, but there will always be many use cases with specific requirements that are not covered by such extension profiles.

RED ALERT LABS
IoT Security

Chapter 4

Use of standards

Use of standards

Terminology

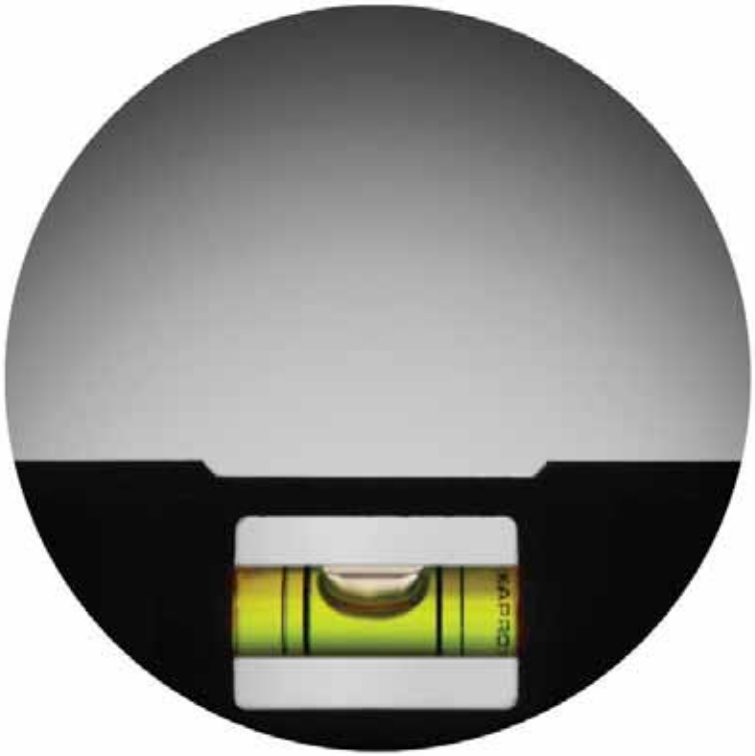
- ISO/IEC 22123-1
- ISO/IEC 17000
- ISO/IEC 9000
- ISO/IEC 27000

Use of standards

EUCS service requirements are defined in an Annex A

- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27017
- documents previously issued by Member States to define the security controls and associated requirements in their respective National Schemes [C5, SecNumCloud, ZekerOnline]

Use of standards



Definition of Evaluation levels

ISO/IEC 15408-3 (Common Criteria)

Use of standards

Conformity assessment methodology

- Based on the ISO/IEC 17065 harmonized standard,
- Will be complemented by additional requirements for the accreditation of CABs that are under development in collaboration with CEN-CENELEC.

Use of standards

Requirements for CABs performing vulnerability identification and penetration testing

- ~~Based on ISO/IEC 17025 harmonized standard.~~ **Also ISO/IEC 17065**
- Complemented by additional requirements for the accreditation of CABs performing these activities, to be developed later as guidance by ENISA in collaboration with the ECCG.

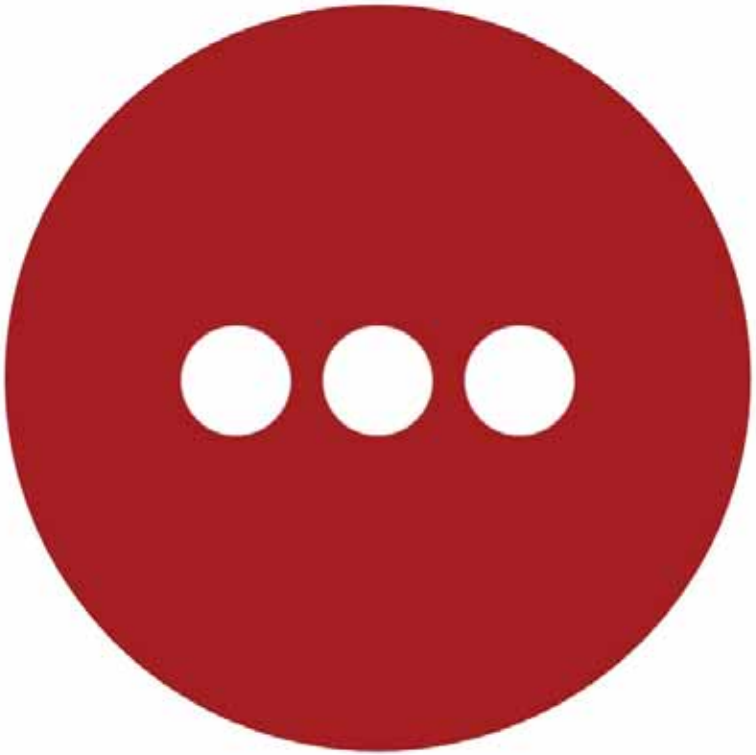
RED ALERT LABS
IoT Security

Use of standards

Conformity assessment methods

- ISO/IEC 17021-1
- ISO/IEC 27006.
- ISAE 3402
- ISAE 3000

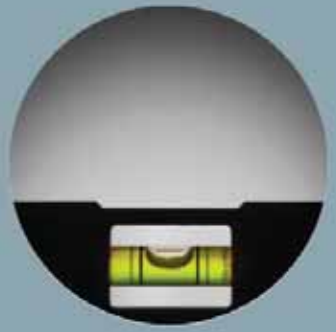
Use of standards



Others references

- Vulnerability handling (ISO/IEC 29147 and ISO/IEC 30111)
- Risk Management (ISO/IEC 27005)

RED ALERT LABS
IoT Security



Chapter 5

Assurance level

CSA

Assurance level

Reminder

EUCSA's Article 52

Basic

Assurance level 'basic' provides assurance that the ICT products, services and processes 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 cyber incidents and cyberattacks.**

Substantial

Assurance level 'substantial' provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level **intended to minimise cybersecurity risks, cyber incidents and cyberattacks carried out by actors with limited skills and resources.**

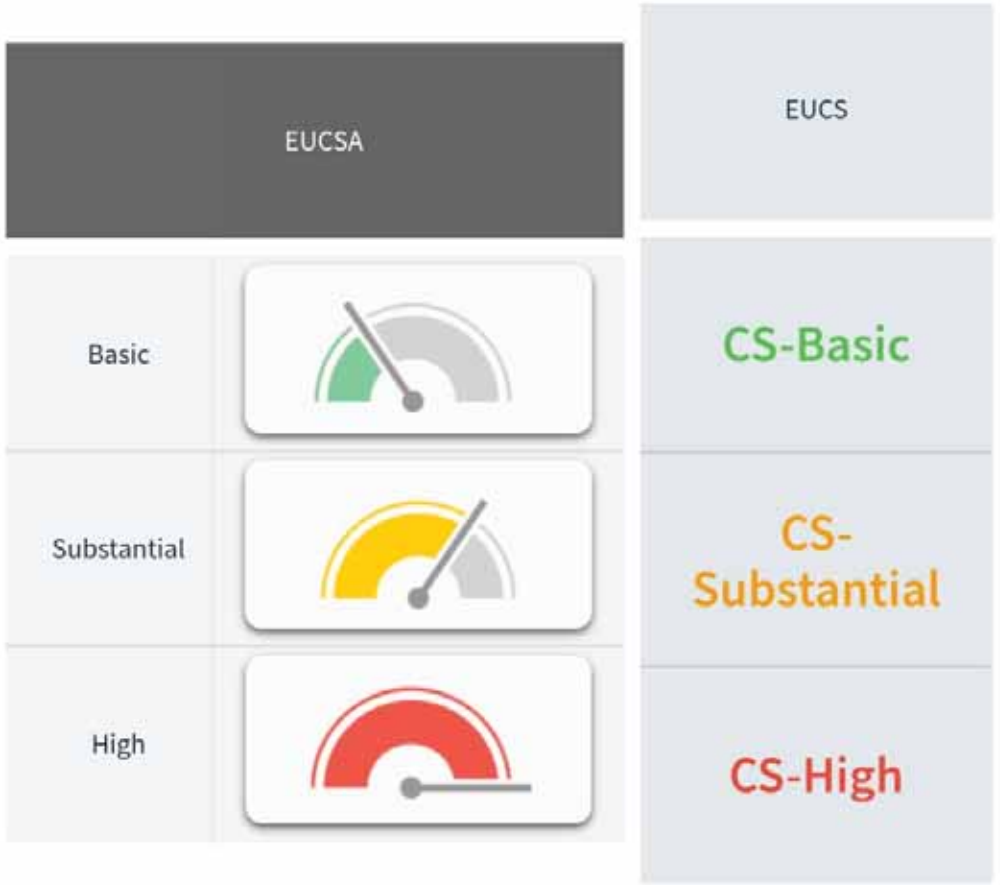
High

A European cybersecurity certificate referring to assurance level 'high' provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level **intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.**

RED ALERT LABS
IoT Security

Assurance levels

The EUCS support the three assurance levels defined in the EUCSA



RED ALERT LABS
IoT Security

Question time

- **Question #1**
  Could you name 2 stakeholders involved in the production of EUCS certificate?

- **Question #2**
  Could you name 1 stakeholder involed in the consumption of EUCS certifiate?

- **Question #3**
  True or False. The ongoing version of the EUCS scheme contain 3 assurance levels directly mapped to the EUCSA.

RED ALERT LABS
IoT Security

Answer

- ✔ Could you name 2 stakeholders involved in the production of EUCS certificate?
  - CSP, CAB, NAB, NCCA, ENISA
- ✔ Could you name 1 stakeholder involed in the consumption of EUCS certifiate?
  - CSC, CSU, Regulatory authorities
- ✔ True or False. The ongoing version of the EUCS scheme contain 3 assurance levels directly mapped to the EUCSA.
  - True. The actual version contain3 evaluation levels CS- Basic, CS-Substantial and CS-High

RED ALERT LABS
IoT Security

CSA

Assurance level

Parameters

Intention	•The intention provides a **general description of the Assurance Level**, most likely matching quite **closely the definition from the EU CSA**.
Suitability	•Suitability is about **potential restrictions** of the types and categories that may be covered.
Attacker profile	•The **attacker profile** cannot be very specific, because of the great **variety of attackers**, and it always defines a wide category of attackers.
Scope of the Evaluation	•The scope of the evaluation should comprise the **service provided by the CSP** and **clearly identify all underlying and supporting services and processes**.
Depth	•The general principle is to follow an **incremental approach**, *i.e.*, that **all requirements of a lower level are similarly included in the depth of the higher level**.
Rigour	•This is about **requiring more structure in the service** (for instance, a security model based on a specific formalism/method) or adding **more structure to the assessment** (for instance, requiring a specific method to collect evidence or provide results).

RED ALERT LABS
IoT Security

EUCS

Evaluation level

	CS-Basic	CS-Substantial	CS-High
Intention	limited assurance through a review by an independent third party that the cloud service is built and operated with procedures and mechanisms to meet the corresponding service requirements at a level intended to minimize the known basic risks of incidents and cyberattacks.	Same than CS-Basic but for minimize the known basic risks of incidents and cyberattacks by actors with limited skills and resources. + implement control to minimise	Same than CS-Substantial but for minimize the risks of state-of-art cyberattacks by actors with significant skills and resources. + implement control to minimise and monitor those continuously
Suitability	Suitable for cloud service that are designed to meet typical security requirements on services for non-critical data and systems.	Suitable for cloud service that are designed to meet typical security requirements on services for business-critical data and systems.	Suitable for cloud service that are designed to meet specific (exceeding evaluation level CS-Substantial) security requirements on services for mission critical data and systems.
Attacker Profile	Single person with limited skills repeating a known attack with limited resources, not including the ability to perform social engineering attacks.	Small team of persons with hacking abilities and access to a wide range of known hacking techniques, including social engineering, but with limited resources, in particular to launch wide attacks or to discover previously unknown vulnerabilities.	Team of highly skilled persons with access to significant resources, possibly including the resources of a third country, to design and perform attacks, get insider attacks, discover or buy access to previously unknown vulnerabilities.

RED ALERT LABS
IoT Security

EUCS

Evaluation level

	CS-Basic	CS-Substantial	CS-High
Scope	Processes and the software underlying the service and meeting "basic" controls	Demonstration of operating effectiveness of the "substantial" controls	Demonstration of operating effectiveness of the "High" controls
Penetration testing	✖	✔	✔
Depth	Document review solely, based on a check for completeness and coherence of the provided internal audit results and of the associated documentation	CS-Basic + On site audit (interview + samples inspection)	CS-Substantial + More verification, more specifics
Rigour	An internal audit is performed by the CSP and driven by a predefined checklist. + An accredited third-party then audits the internal audit report and its supporting documentation.	The evaluation is performed by an accredited third-party, and it is driven by a risk analysis performed by the CSP, which is in the audit scope.	CS-Substantial + CAB is authorised by a NCCA + More rigour is expected

RED ALERT LABS
IoT Security

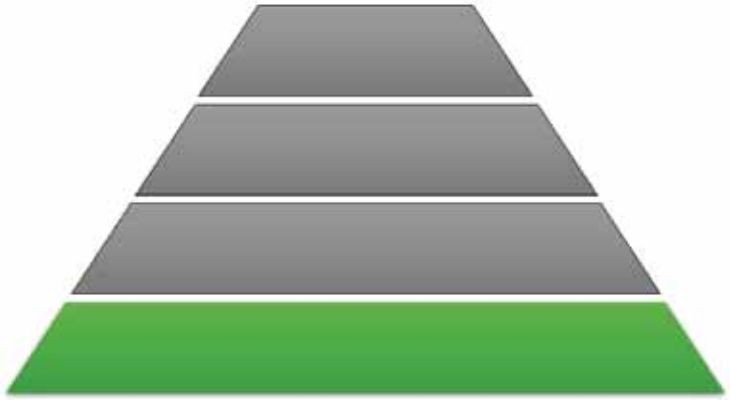
Operating Effectiveness over a period of time

Frequency of the control	Assumed population of control occurences	Sample Size (per specified Period)
More than daily	Over 250	25-60
Daily	250	20-40
Weekly	52	5-15
Monthly	12	2-5
Quarterly	4	2
Annually	1	1

RED ALERT LABS
IoT Security

Evaluation level

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



CS-Basic

- Every evaluation level is commensurate with the level of **risk associated to the intended use of the cloud service**, as demonstrated in the definition of **suitable** services and typical **attacker profiles** (Article 52(1)).
- Every **evaluation level defines assurance components as service requirements**, as well as **the rigour and depth required in the evaluation** (Article 52(3)).
- Every evaluation level requires that evaluation activities **include a review of technical documentation** (Article 52(5), Recital 67).
- Every evaluation level requires a review of **the cloud service's main processes, including the development process used for the development of the cloud service** (Recital 88)

RED ALERT LABS
IoT Security

Evaluation level

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

CS-Substantial

- The requirements on security controls for **assurance level 'substantial' include a vulnerability assessment activity that performs a review of publicly known vulnerabilities** (Article 52(6)).
- The requirements on security controls for assurance level 'substantial' **include a review of the functional tests of the cloud service's security functionalities as well as some independent testing requirements** (Article 52(6)),
- The assessment methodology for assurance level '**substantial**' **mandates the review of a mapping between the documentation of security functionalities and their implementation to ensure compliance** (Recital 89).

RED ALERT LABS
IoT Security

Evaluation level

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

CS-High

- The requirements on security controls for assurance level **'high' include a vulnerability assessment activity that performs a review of publicly known vulnerabilities** (Article 52(7)).
- The requirements on security controls for **assurance level 'high' include a review of the functional tests of the cloud service's security functionalities, as well as automated monitoring requirements,** (Article 52(7)).
- The requirements on security controls for **assurance level 'high' include the correct implementation of the necessary security functionalities at state-of-the-art (Article 52(7)).**
- The assessment methodology for assurance level 'high' mandates the **review of a full mapping between the documentation of security functionalities and their implementation to ensure compliance** (Recital 89).
- The assessment methodology for **assurance level 'high' mandates design effectiveness and operating effectiveness to be assessed during the evaluation** (Recital 90). This assessment includes **penetration testing to assess the resistance of security functionalities of the cloud services; in addition, some of the penetration testing shall be performed by an accredited and authorised entity** (Article 52(7), Recital 90).

RED ALERT LABS
IoT Security

Chapter 6

EU Statement of conformity

EUCS

EU Statement of conformity

- Could only have been allowed for CS-Basic(low risk CSP)

  The Ad Hoc Working Group consistently expressed that self-assessment was not suitable for cloud services, even at level CS-Basic and even on a strictly defined subset of services.

- **NOT ALLOW**

  Although divergent opinions have been expressed, in particular in the surveys performed over the summer of 2020, ENISA has decided to follow the recommendation of the AHWG and to not allow the issuance of EU statements of conformity in the initial version of this scheme, as there are enough challenges to be met in that first version.

- Reconsideration possible

  This decision may be reconsidered in future releases of the EUCS, in particular after evaluating the quality of the work performed by CSPs on the internal audits that are used as a basis for the conformity assessment at CS-Basic.

RED ALERT LABS
IoT Security

Chapter 7

Specific requirements applicable to CAB

EUCS

CABs

CAB ? CB ? ITSEF ?

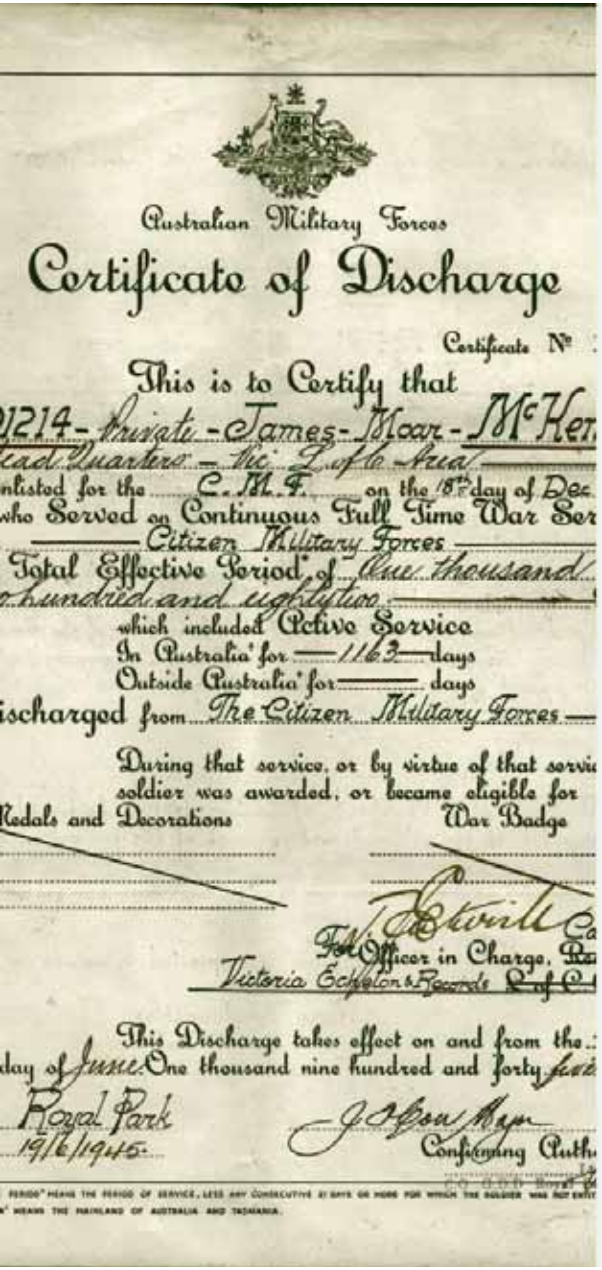
The EUCS does not distinguish between the roles of Certification Body and Evaluator, like EUCC does.

Therefore, for the evaluation level CS-high, no specific accreditation (17025) is required to perform evaluation activities related to vulnerability identification and penetration testing.

Nevertheless, personnel performing test activities shall have the necessary expertise to perform specific testing activities.

No need to be accredited according to ISO/IEC 17025 to perform penetration testing, a CAB accredited according to ISO/IEC 17065 can do it.

RED ALERT LABS
IoT Security


Australian Military Forces
Certificate of Discharge
Certificate No
This is to Certify that
1214 - Private - James - Moar - McKen
ead Quarters - Vic L of C Area
nlisted for the C.M.F. on the 18th day of Dec
who Served on Continuous Full Time War Ser
Citizen Military Forces
Total Effective Period of One thousand
hundred and eightytwo
which included Active Service
In Australia for 1163 days
Outside Australia for days
ischarged from The Citizen Military Forces
During that service, or by virtue of that servi
soldier was awarded, or became eligible for
Medals and Decorations War Badge
For Officer in Charge,
Victoria Echelon & Records
This Discharge takes effect on and from the
day of June One thousand nine hundred and forty five
Royal Park
19/6/1945
Confirming Auth

CAB issuing certificate

Needs

CS-High

Accredited

According to ISO/IEC 17065.

Notification

Meet additional requirements defined for EUCS

Authorisation

Because the evaluation activities will include additional competences like strong technical competences.

RED ALERT LABS
IoT Security

Chapter 7

Additional requirements for CS-high (Chapter 7)

Specific requirements to which CABs are subject

- specific requirements concern technical competences related to specific conformity assessment activities **(for CS-high certificate)**;
- requirements shall apply both to internal personnel of CABs and to the external ones in cases where conformity assessment activities are performed by a subcontractor.

These CABs and their concerned personnel shall :

- have the necessary expertise and experience in designing and performing pentests
- have the necessary expertise and experience in performing reviews of the design and implementation of security measures in cloud service.

RED ALERT LABS
IoT Security

EUCS - Chapter 7 - Specific requirements applicable to CAB

Annex C

Requirement for all levels

- ISO 17065 + additional requirements specific to the EUCS, to be defined in a separate document.

Requirement for CS-high

- ISO 17065 + additional requirements specific to the EUCS, to be defined in a separate document.
- Technical requirements related to
  - Reviews of the architecture and of the configuration of a cloud service's system components;
  - Reviews of the CSP's source code and related documentation;
  - Penetration testing of the controls implemented to satisfy the audit criteria, including the EUCS service requirements.
- Skills inspired from [PASSI- qualification of security audit providers], should be considered for inclusion in the required skills for evaluation team
  - networks and protocols, security equipment and software, OS, cloud computing, application layer, attacks
- Penetration tester should be able to :

  • Develop codes, scripts and programmes • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Identify and solve cybersecurity-related issues • Communicate, present and report to relevant stakeholders • Use penetration testing tools effectively • Conduct technical analysis and reporting • Decompose and analyse systems to identify weaknesses and ineffective controls • Review codes assess their security

RED ALERT LABS
IoT Security

EUCS - Chapter 7

CABs

Authorisation

The development of a Technical Specification is ongoing in WG3 of JTC13 in order to define requirements for the accreditation of CABs who will issue certificates in the context of the EUCS

TS 18072

NCCA shall

- for the authorisation of a CAB to carry out activities at evaluation levels CS-high under the EUCS scheme, proceed to the assessment of the compliance with the additional requirements, including any of its subcontractors performing evaluation activities

This assessment shall include :

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

RED ALERT LABS
IoT Security

EUCS - CAB competences

Preview of the document under construction (TS18072)

Annex A – Required Knowledge and Skills

	Evaluator	Evaluator leading the evaluatio	Evaluation team	Personnel conducting the appl review to determine the evalua team competence required, to the evaluation team members a	Personnel reviewing evaluation reports and making certificatio decisions
GENERAL	See A.2.1	See A.2.1	See A.2.1		See A.5.1
knowledge of cybersecurity	X	X			X
technical knowledge of Cloud Services			X		
knowledge of management systems for the provision of information technology services	X	X			
knowledge of the principles of evaluation including auditing	X	X			
knowledge of service monitoring, measurement, analysis and evaluation	X	X			
evaluation processes and procedures		X			X
evaluation principles, practices and techniques		X			X
INFORMATION SECURITY TERMINOLOGY, PRINCIPLES, PRACTICES AND TECHNIQUES	See A.2.2	See A.2.2	See A.2.2		See A.5.2
cybersecurity specific terminology and documentation structures, hierarchy and interrelationships	X	X	X		X

Categories covered

- General
- Information security terminology, principles, practices and techniques
- Certification scheme-specific standards and normative documents
- Business management practices
- Client's business sector
- Client's products, processes and organization
- Team leadership

RED ALERT LABS
IoT Security

Question time

- **Question #1**

  Could you list 3 parameters that are used in the definition of the evaluation levels of the EUCS?

- **Question #2**

  True or False. Is EU Statement of conformity allowed in the context of the EUCS?

RED ALERT LABS
IoT Security

Answer

- ✔ Could you list 3 parameters that are used in the definition of the evaluation levels of the EUCS?
  - Intention, Depth, Rigour, Attacker profile, Suitability, Scope of Evaluation
- ✔ True or False. Is EU Statement of conformity allowed in the context of the EUCS?
  - False. But this could be reconsidered for CS-Basic when it is proven how CSP operates.

RED ALERT LABS
IoT Security

Reminder this morning

"Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning."

EINSTEIN

1 | Cloud Security Introduction

2 | Introduction to EUCS Scheme

3 | Deep-dive into EUCS

- PURPOSE OF THE SCHEME
- USE OF STANDARDS
- ASSURANCE LEVELS
- EU STATEMENTS OF CONFORMITY
- SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

Chapter 8

Evaluation methods & criteria

EUCS - Chapter 8 - Evaluation methods & criteria

How to test ? (+ latest version of TS 18072:2024)

Test according to criteria defined in Annex A - TS 18026

Use the assessment methodology defined in Annex B

Take into account the additional elements of the harmonised interpretation developped by ENISA (to come)

RED ALERT LABS
IoT Security

This categories covered all the security objectives mentionned in Article 51 of the EUCSA

What should be tested ? (+ latest version of TS 18026)

Annex A - Security controls

RED ALERT LABS
IoT Security

What should be tested ? (+ latest version of TS 18026)

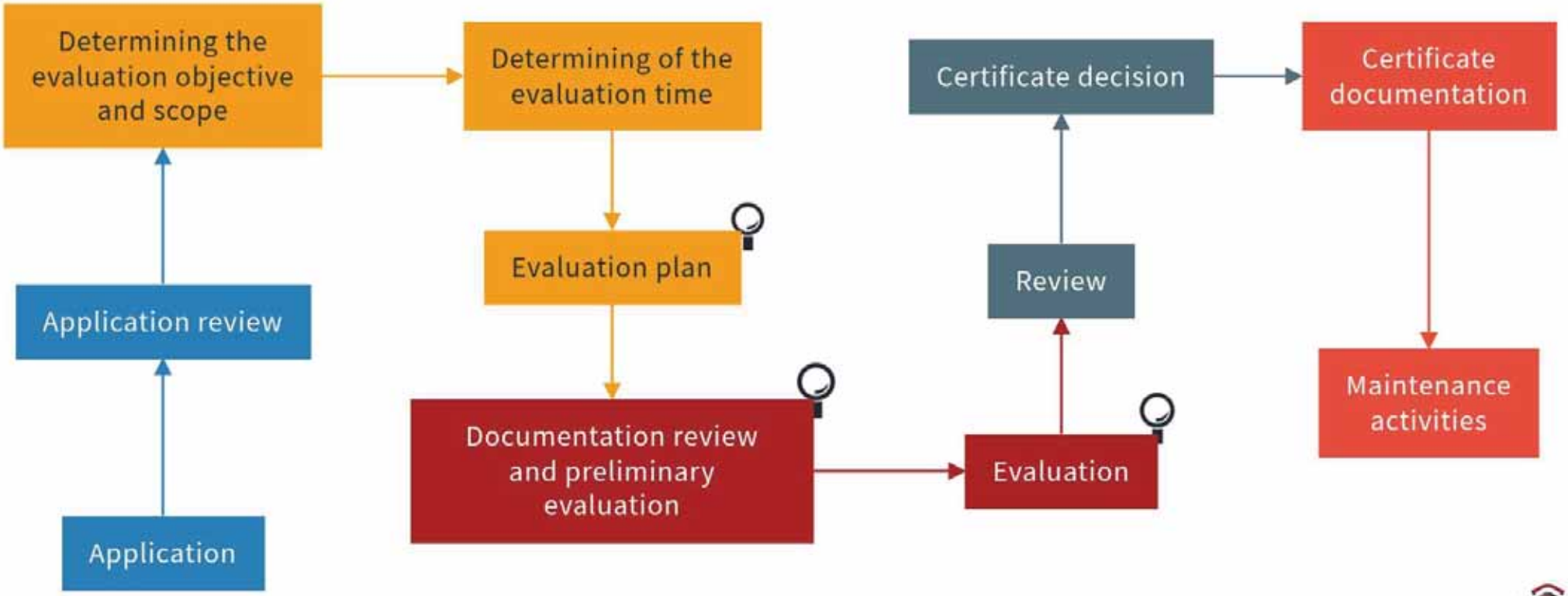
Annex A - Security controls - Example

Basic	**The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least:** • **Non-reuse of credentials;** • **Trade-offs between entropy and ability to memorize;** • **Recommendations for renewal of passwords;** • **Rules on storage of passwords; and** • **Confidentially of personal (or shared) authentication and non-sharing of credentials.**	IAM-08.1B	Substantial	The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: • Non-reuse of credentials; • Trade-offs between entropy and ability to memorize; • Recommendations for renewal of passwords; • Rules on storage of passwords; • Confidentially of personal (or shared) authentication and non-sharing of credentials; • **Recommendations on password managers; and** • **Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling.**	IAM-08.1S
	Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01), except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.	IAM-08.2B		Passwords shall be only stored using cryptographically strong hash functions (cf. CKM-01), except when passwords are stored for subsequent re-use in the plain text form, for example in a password manager.	IAM-08.2S
	In the latter case stored passwords shall be protected, using a cryptographically strong mechanism.	IAM-08.3B		In the latter case stored passwords shall be protected, using a cryptographically strong mechanism.	IAM-08.3S
	If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	IAM-08.4B		If cryptographic authentication mechanisms are used, they shall follow the policies and procedures from CKM-01.	IAM-08.4S
				When creating credentials, compliance with policies shall be enforced.	IAM-08.5S

EUCS - Chapter 8 - Evaluation methods & criteria

Certification process

Annex B - approach for the assessment + (Document under construction by TG3)



RED ALERT LABS
IoT Security

Zoom on

"Evaluation plan"

- Describe evaluation activities
- Tailored
- Consider
  A. the competence of the personnel in charge of implementing the controls;
  B. the relevance and reliability of the evidence to be obtained;
  C. the nature of the controls, including their level of automation, and the frequency with which they operate;
  D. the degree to which the controls rely on the effectiveness of other controls.
- Consider also :
  A. the relevance and reliability of the evidence to be obtained;
  B. the nature of the controls, including their level of automation, and the frequency with which they operate;
  C. the degree to which the controls rely on the effectiveness of other controls;
  D. the evaluation level targeted for certification.
- For each evaluation activity, determine :
  A. the target (what is being evaluated);
  B. the nature (what kind of evaluation activity);
  C. the timing (at what point in time or over what period);
  D. the extent (how many or how often to execute the activity).
- Select a sample of test services
- Identify potential vulnerabilities

EUCS - Chapter 8 - Evaluation methods & criteria

Zoom on

"Documentation review and preliminary evaluation" - Evaluation stage 1

- Review the client's service documented information
  evaluate whether those aspects of the description are fairly presented.
- Determine to what extent and for which processes the client uses subservices and how the client controls and monitor the services provided by these subservice providers.
  - determine which evaluation method is appropriate for each subservice
  - identify which subservice organisations do have an acceptable assurance documentation which can be (re)used in the dependency analysis
- Consider the relative importance and effect of possible omissions or deviations
- Evaluate the client's site-specific conditions
- Undertake discussions with the client's personnel
- Review the client's status and understanding regarding the evaluation criteria
- Evaluate if the internal audits and management reviews required by the certification scheme are being planned and performed
- Obtain necessary information regarding the scope of the service
- Provide a focus for planning stage 2 by gaining a sufficient understanding of the cloud service and site operations
- Review the allocation of resources for stage 2 and agree the details of stage 2
- Determine the roles and responsibilities of the evaluation team members
- Document conclusions

RED ALERT LABS
IoT Security

Zoom on

"Evaluation" - Evaluation stage 2

- Verify Suitability of the Design of Controls
  - assessing the completeness and accuracy of the client's identification of risks
  - evaluate the linkage of the controls with those risks
  - evaluate the competence and authority of the persons
  - understand the specific activity to determine especially how the control is triggered, how it is executed, which tools or systems are used to support the execution and which records are kept evidencing the execution;
  - validate the source of information
- Verify Operating Effectiveness
  - Verify that the control is consistently applied as designed
  - in case of manual controls, they were applied by individuals who have the appropriate competence and authority
- Analysis of Results
  - evaluate whether the described technical and organizational controls refer to or describe the evaluation criteria;
  - consider whether the provided information adequately disclose the significant controls;
  - consider whether the controls are deemed suitable to meet the evaluation criteria ;
  - ensure that the information provided appears relevant, reliable, comprehensive and comparable;
  - assess if it can be concluded that nothing has come to its attention that causes evaluators to believe that the technical and organizational manners implemented by the client are not meeting the requirements of the assurance level
- Issuing the Evaluation Report

Chapter 9

Necessary information for certification

EUCS - Chapter 9

Necessary information for certification

What the CSP should provide to the CAB ?

Scope of the target certification

- Targeted assurance level and why.
- Detailed description of the cloud services
- List of Subservices used and
  - controls imposed to them (CSOCs)
- list of Complementary User Entity Controls (CUECs) they provide to their users

Previous evaluation results

in case of composition or renewal.

Demonstration to compliance to the EUCS Security controls (TS 18026)

All the information needed to demonstrate that the implementation of their cloud service meets the evaluation criteria for the targeted assurance level

questionary

proof of compliance (procedures, process, form, records, logs, ...)

Additional information asked by the CAB

Additional information may be required when the conformity assessment is performed

RED ALERT LABS
IoT Security

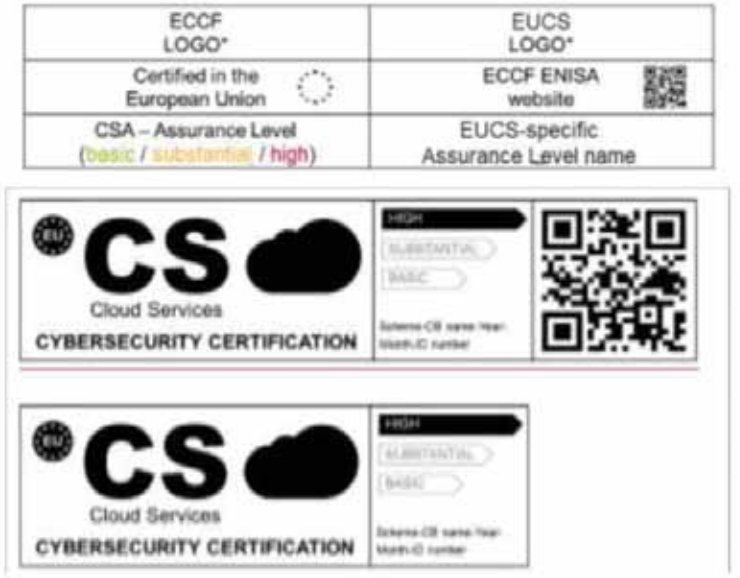
Chapter 10

Marks and Labels

EUCS - Chapter 10

Marks and labels

- Make the certification easily recognizable
- Provide direct link to the information
- Contain summary of information
  - Logos (ECCF and EUCS)
  - QR code
  - Assurance level / EUCS evaluation level
  - "Certified in the European Union"
  - Potential additional information (CSEP, etc...)



RED ALERT LABS
IoT Security

Chapter 11

Compliance monitoring

EUCS - Chapter 11

Compliance monitoring

- A NCCA activity

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

  The implementation of compliance monitoring by NCCAs may be the subject of peer review between NCCAs.

- Cases of non compliance

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

General information

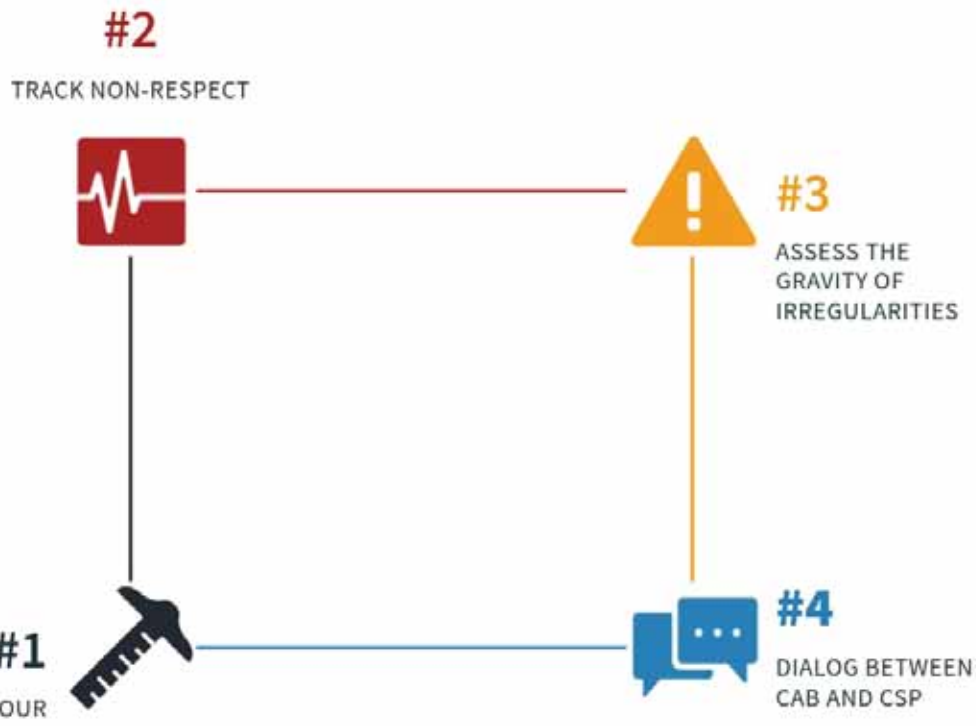
RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

Deviations and irregularities consider as potential **non-compliance by CSP** || How to avoid it ?

- any deviation from the requirements applicable to the information supplied to a CAB, discover after the certification
- any deviation from the requirements regarding the certificate content and the supplementary cybersecurity information
- any deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity



Rigourous certification process

RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

Potential non-compliance **by CAB** || How to avoid it ?

Failure to meet obligation:

- obligations for auditing the scheme compliance
- obligations for supervising
- obligations for complaint handling
- ...

Test

- the audits ;
- the permanent monitoring of the CAB by their Accreditation bodies
- monitoring of CAB's subcontractors by the CAB and their Accreditation bodies.

Deviations from evaluation requirements

- Unjustified deviations from the evaluation methodology
- deviations from expected evaluation competence.
- ...

Detect

through the quality process of the CAB, including the report to the NCCA of the identified issue, and the requirement to handle complaints associated to their accreditation.

RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

Potential Nonconformity of a certified cloud service || How to avoid it ?

Potential Non conformities :

- a change in the certified cloud service itself leading to a change of the cloud service's security posture;
- a significant security incident that has impacted the certified cloud service;
- a change in the threat environment;
- a vulnerability identified.

CSP

- inform their CAB of major changes;
- monitor vulnerabilities;
- monitor the known dependencies and vulnerabilities identified by any other source
- inform the CAB of any significant security incident
- work in cooperation with the CAB and where necessary with **the NCCA** to support their monitoring activities.

CAB

- monitor vulnerabilities that would be relevant to their clients' scope
- monitor the handling of security incidents reported by CSPs
- report to their NCCA any detected vulnerability affecting the conformity of a certified cloud service

RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

The sampling

- shall be based on sampling
- using generic parameters
  - Cloud service capabilities,
  - assurance level,
  - CSP,
  - CAB,
  - any information brought to the the knowledge of the NCCA as :
    - complaints,
    - security events,
    - etc...

Sample annually a minimum of 5% of the cloud services which have been the subject of a successful conformity assessment in the context of the EUCS scheme in the previous year

and at least one cloud service per annum.

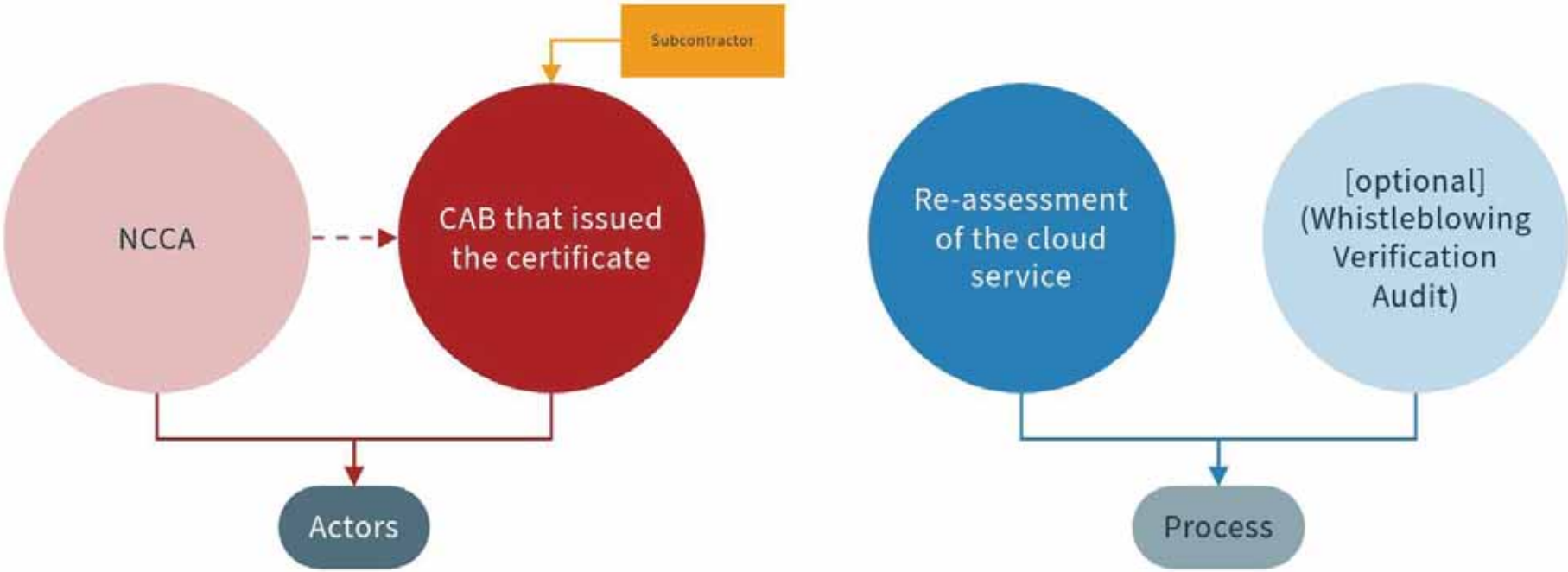
The CSP shall be informed of the selection reasons

RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

The Monitoring



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

RED ALERT LABS
IoT Security

EUCS - Chapter 11 + Annex E.2

Compliance monitoring

The CSP shall support re-assessment activities as they supported the original conformity assessment activities, including financial support.

The re-assessment

NCCAs are required in the context of the compliance monitoring process to perform a number of re-assessments every year, depending on the number of certificates issued or maintained during the previous year.

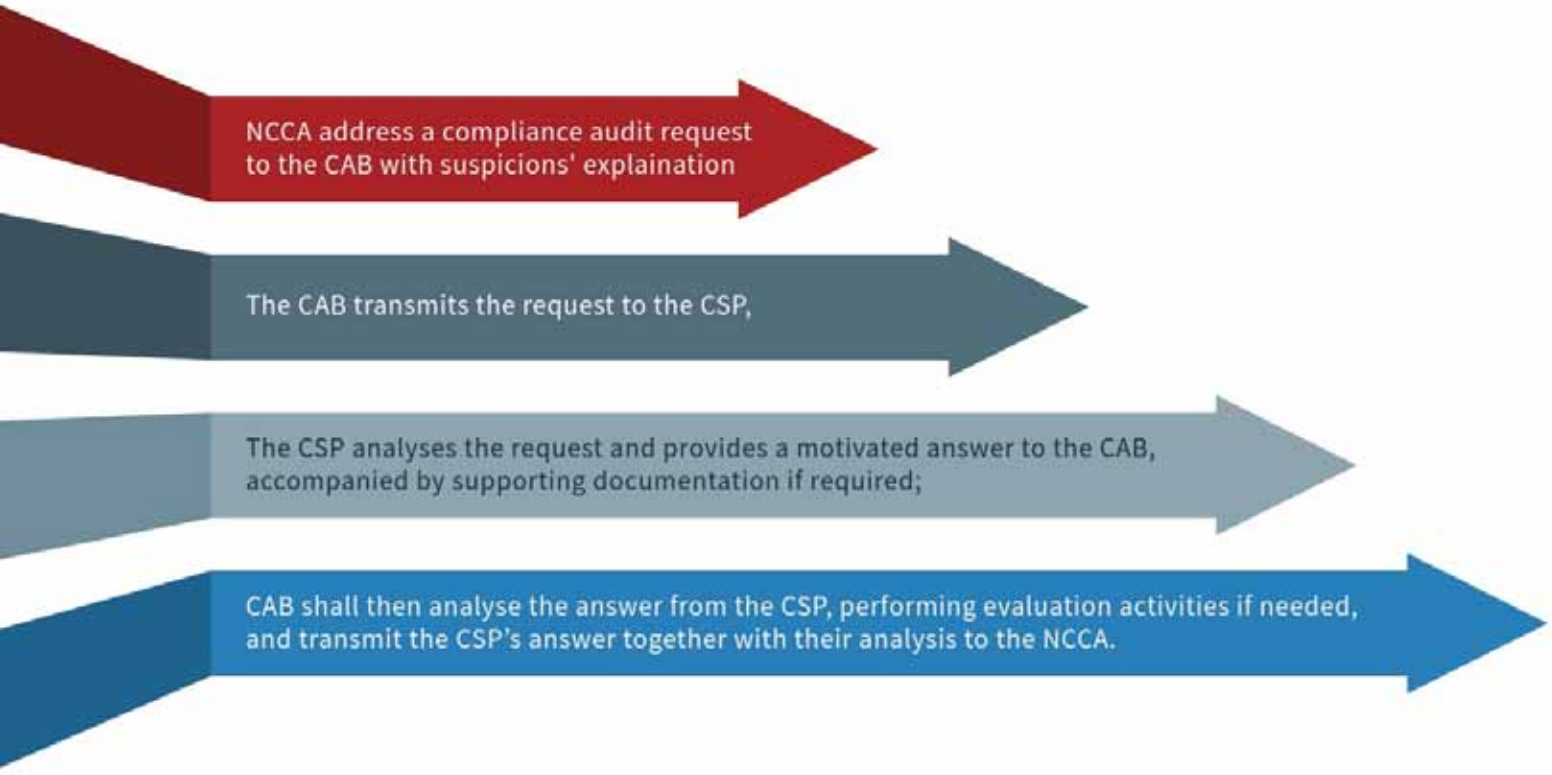
CAB send documentation	Contact with the CSP	Request additional information	Verdict
make available to the NCCA all the documentation that was available to CABs at the time of the review and certification decision.	As needed for their re-assessment, the NCCA may contact the CSP in order to be granted access to the documents for which they have only provided restricted access to the CAB during the audit.	• request additional information and explanations from the CAB; • have the CAB perform the activity again, possibly while monitored by a NCCA representative; • have a NCCA representative perform the activity again.	

RED ALERT LABS
IoT Security

EUCS - Chapter 11 + Annex E.2

Compliance monitoring

Compliance audit (Whistleblowing Verification)



If the CAB does not confirm the CSP's analysis, then the NCCA shall take the final decision after consulting both parties

RED ALERT LABS
IoT Security

EUCS - Chapter 11 + Annex E.2

Compliance monitoring

Vulnerability assessments

1 Potential vulnerability identification

When they become aware of a vulnerability that may affect a certified cloud service, the CAB shall request a vulnerability assessment from the CSP. This may happen in particular when the NCCA requests the CAB to investigate a vulnerability.

2 Transmission to the CSP

The CAB transmits the request to the CSP

3 CSP Analysis and plan

The CSP analyses the request.

Provides a motivated answer to the CAB, with the status of infection, the severity of the vulnerability, the mitigation plan and supporting documentation ;

4 CAB Analysis

The CAB analyses the answer from the CSP, performs evaluation activities if needed, and if applicable, transmits the CSP's answer with their analysis back to the NCCA.

5 NCCA verdict

If the CAB does not confirm the CSP's analysis, then the NCCA shall take the final decision after consulting both parties.

RED ALERT LABS
IoT Security

EUCS - Chapter 11 + Annex E.2

Compliance monitoring

CAB Audits

- If the NCCA that authorized a CAB or the NAB that accredited a CAB have doubts about the conformity of the CAB to their accreditation or authorisation requirements, the relevant authority shall engage with the CAB to perform all necessary verifications, including any conformity assessment activity that is required.
- The NCCA and NAB should coordinate their actions when such situations occur.

RED ALERT LABS
IoT Security

EUCS - Chapter 11

Compliance monitoring

Force majeure

What is a case of "force majeure" ?

A major event affect the validity of lot of certificate worldwide in the same time.

(spectre, meltdown, log4j, ...)

Who shall take action ?

Impacted NCCA

What should be done ?

- Ensure continuity of certification
- Inform ECCG about the force majeure measures
- Coordinate with other affected NCCAs
- Inform ENISA about extension of certificate if any

RED ALERT LABS
IoT Security

Question time

- **Question #1**
  What are the 3 types of non compliance define by the scheme ?
- **Question #2**
  Name 3 monitoring activities described in this section ?
- **Question #3**
  True or False. Is “force majeur” manage by the CABs ?

RED ALERT LABS
IoT Security

Answer

- What are the 3 types of non compliance define by the scheme ?
  - CSP, CAB, certificate non-conformity, vulnerability assessment
- Name 3 monitoring activities described in this section ?
  - Re-assessment, CSP Compliance audit, CAB audit
- True or False. Is “force majeur” manage by the CABs ?
  - False. This is manage by NCCA

RED ALERT LABS
IoT Security

Chapter 12

Certificate Management

EUCS - Chapter 11 + 12 + Annexe E

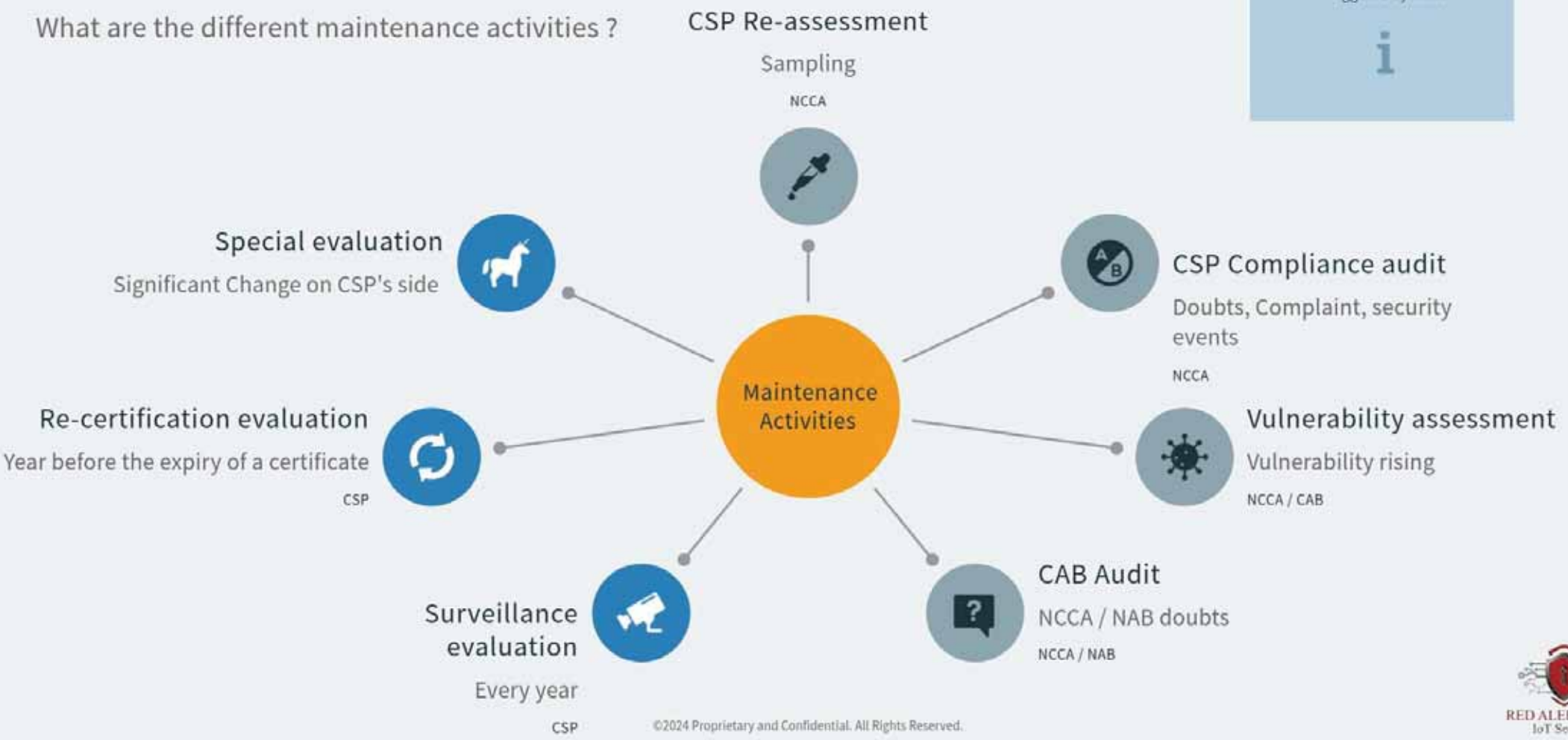
Certificate maintenance

What are the different maintenance activities ?

Type of activity

Triggered by what?

Triggered by who?



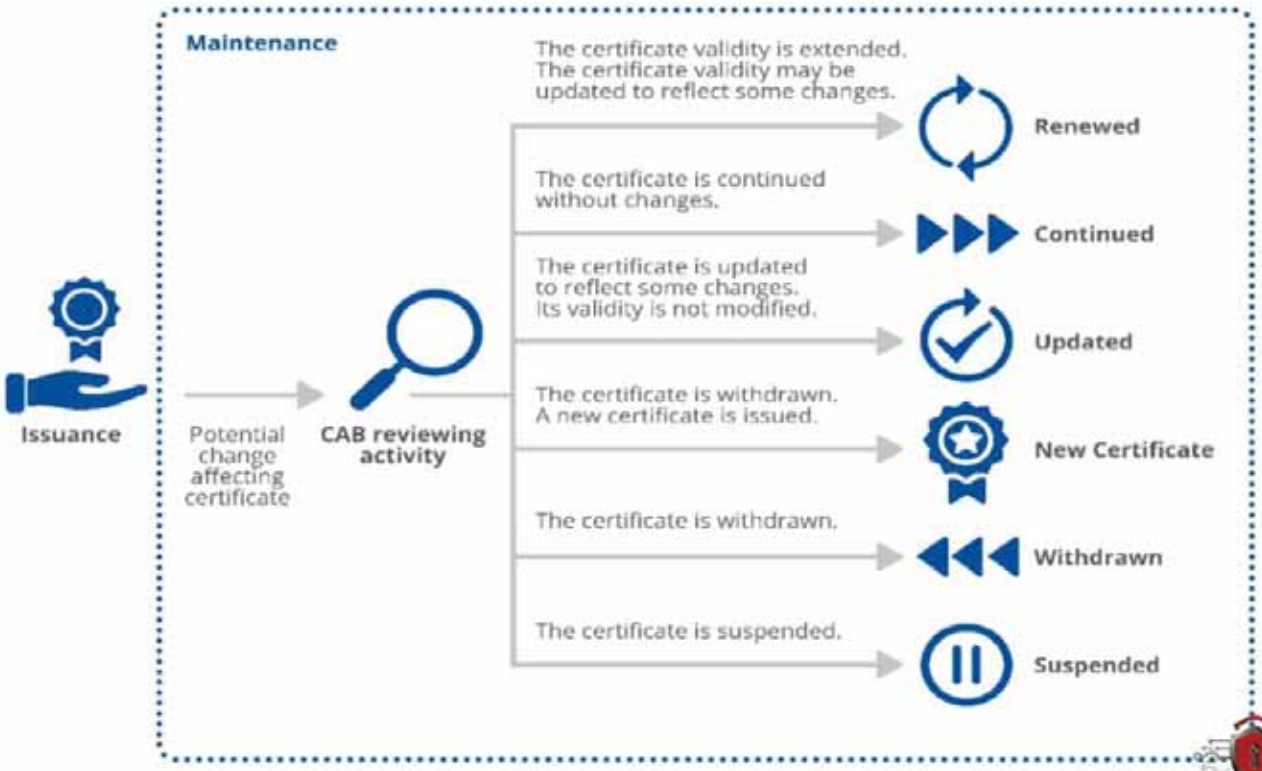
RED ALERT LABS
IoT Security

EUCS - Chapter 12

Certificate maintenance

What can happen to a certificate?

- Based on ISO/IEC 17065
- After Maintenance activities
- Upon review and decision of the CAB, the maintenance activities shall result in one these decisions ➡

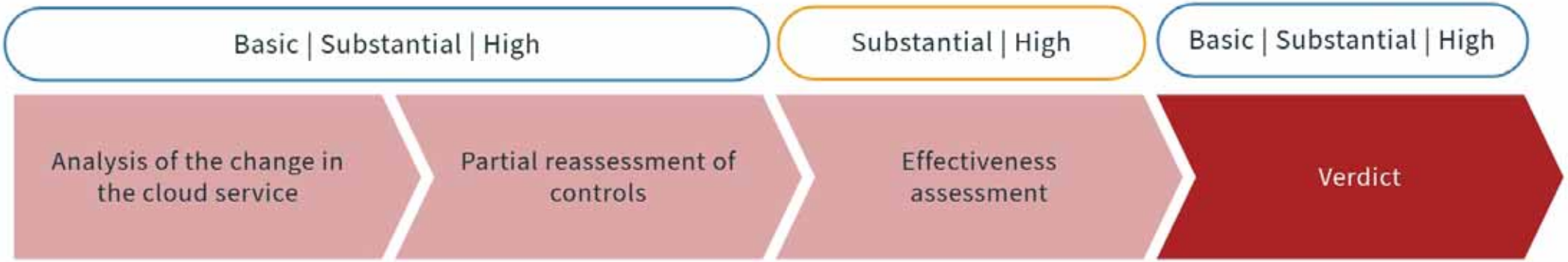


RED ALERT LABS
IoT Security

EUCS - Chapter 12

Surveillance evaluation

Process



- Obtain an understanding of the changes operated.
- Determine a list of affected controls.
- Assess the suitability of the design of the modified controls.
- Assess the existence and implementation of the modified controls.

- Select a subset of controls, including at least the controls for which observations were made in the previous conformity assessment,
- Assess the suitability of the design of the selected controls.

- Assess the operating effectiveness of controls (all for CS-High and half for CS-Substantial) over the period since the previous assessment of operating effectiveness.

RED ALERT LABS
IoT Security

EUCS - Chapter 12

Special evaluation

A special assessment may also be triggered by a CSP at any time, typically after performing significant changes to their cloud service or to their control framework

Analysis of the change in the cloud service

- Obtain an understanding of the changes.
- Determine a list of affected controls,
- Assess the suitability of the design of the affected controls;
- Assess the existence and implementation of the affected controls;
- Determine whether the changes on the affected controls are sufficient to fulfil all the EUCS requirements.

Effectiveness assessment

- Assess the operating effectiveness of affected controls over the period since the previous assessment of operating effectiveness.

RED ALERT LABS
IoT Security

EUCS - Chapter 12

Re-certification evaluation

Process

When?

in the year before the expiry of a certificate

How?

Alike an initial assessment, a re-certification assessment of a cloud service shall cover all parts of the conformity assessment methods.

+ re-use previous result

Why?

extend certificate's validity for another 3-year period

RED ALERT LABS
IoT Security

EUCS - Chapter 12

Certificate maintenance

Typical certificate life-cycle

RED ALERT LABS
IoT Security

Chapter 13

Non compliance

EUCS - Chapter 13

Non-compliance

What happens when a **CSP** non-compliance is suspected ?

CAB who issued the certificate :

- investigates, and if deviation confirmation :
  - Requests the CSP assertions and amendments to restore compliance

Continued non-compliance past the allowed time frame trigger a suspension of the certificate for the cloud service and suspension of all current certification process of the CSP.

+ Inform NCCA / ENISA of the suspension

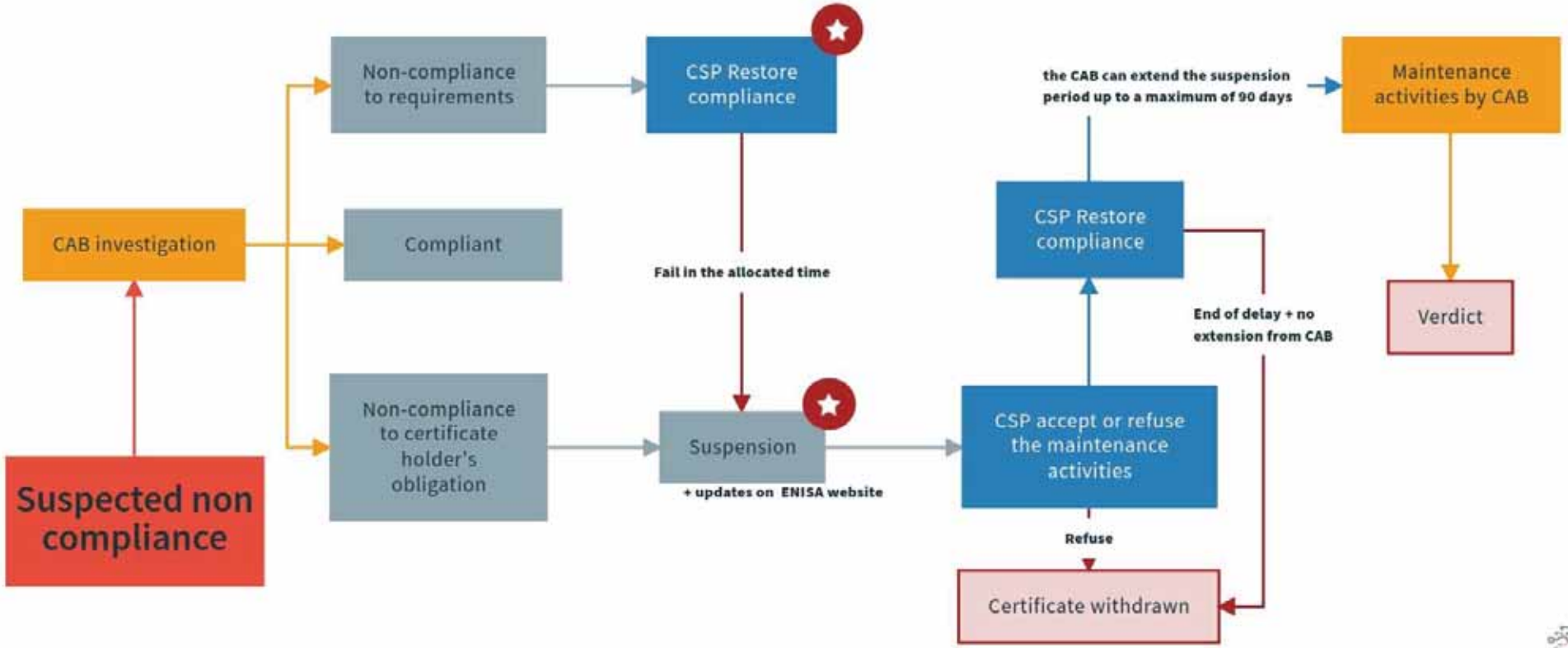
The CSP shall support re-assessment activities as they supported the original conformity assessment activities, including financial support.

RED ALERT LABS
IoT Security

EUCS - Chapter 13

Non-compliance

What happens when a CSP non-compliance is suspected ?



RED ALERT LABS
IoT Security

EUCS - Chapter 13

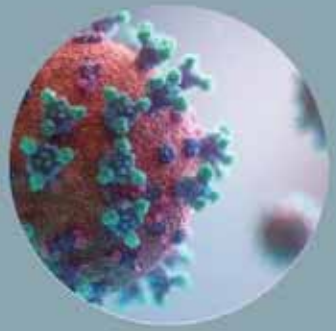
These activities shall be support by the CAB, including financial support if needed

Non-compliance

What happens when a **CAB** non-compliance is suspected ?

RED ALERT LABS
IoT Security

A



Chapter 14

New Vulnerabilities

Towards a Guidance Document

EUCS
Vulnerability Management

Chapter 14 of the EUCS Scheme

RED ALERT LABS
IoT Security

Vulnerability Handling

- CSPs shall use the general steps of ISO/IEC 30111 for vulnerability handling

  Preparation, receipt, verification, remediation development, release, post release, with specific application rules for the EUCS

- Application rules for the EUCS

  These rules are defined in the chapter 14, as well as in the definition of the security controls related to security incident management, in Annex A: (Security Objectives and requirements for Cloud Services).

1- Preparation

- Develop methods for receiving vulnerability information

  These methods shall be made public as per Article 55.1.c of the CSA.

RED ALERT LABS
IoT Security

2- Receipt

Use Cases

CSP of the certified cloud service receives vulnerability information according to Article 55.1.(c) of the EUCSA

New publicly disclosed vulnerability on the referenced online repositories according to Article 55.1.(d) of the EUCSA;

CSP finds out a related vulnerability to its certified cloud service in any other way

RED ALERT LABS
IoT Security

2- Receipt

Handling Vulnerability

According to the CSP's defined policies and procedures.

- ✔ If the vulnerability analysis determines that the risk related to the vulnerability is major

  Then the CSP shall report without delay to the CAB that issued the certificate a description of the vulnerability, together with a description of its impact

The time between the moment the CSP learns about the vulnerability and the notification of the CAB

- shall not exceed **seven (7) working days**

Failure to notify the CAB of a vulnerability with potential major impact or to do so within the delays defined above shall be considered as a non-compliance to the rules of the scheme, as defined in Chapter 13 (NonCompliance)

RED ALERT LABS
IoT Security

2- Receipt

Handling Vulnerability

At the time the CSP notifies the CAB, the analysis of the vulnerability may not be finalized.

CSP shall provide to the CAB a date for the delivery of the full analysis without undue delay.

Type of information to share

- ✔ possible exploit(s) of the vulnerability

  In that case, it shall carry the appropriate **TLP classification** as to ensure the relevant protection, in accordance with the standard rules defined in https://www.first.org/tlp/, or **with alternative classification** and mechanisms previously agreed between the CSP and the CAB.

RED ALERT LABS
IoT Security

3- Verification / 4-Remediation Development

In its analysis of the vulnerability with major impact, the CSP shall propose

1. whether or not the certificate should be suspended until a remediation is released
2. whether or not a special conformity assessment should be performed on the cloud service after remediation

The CAB shall approve the proposed actions or make alternative proposals within **seven (7) working days.**

If no decisions ==> inform the NCCA and ask for its advice, and if required for additional delays

If a special conformity assessment has been deemed necessary

It shall be performed before lifting a potential suspension of the certificate

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

5- Release and Post Release

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

Vulnerability Disclosure

Not longer than 90 days embargo on vulnerability disclosure

- Certificate holders can impose three (3) months embargo on vulnerability disclosure, extendable with NCCA approval, to limit disclosure to certain parties.
- CSPs could decide to disclose the vulnerability to some or all of CSCs

Notify and share vulnerability details

- Certification bodies must notify NCCAs of confirmed vulnerabilities
- Only necessary information to understand the impact of the vulnerability.
- Maintaining confidentiality of exploitation details (e.g no details about exploits)

NCCA shall share information with other NCCAs

- Could ask for further investigation for CABs
- Information exchange shall be done in confidentiality, including application of encryption and need-to-know principle .

Embargo, notification, and public disclosure guidelines for vulnerabilities found in certified solutions.

Vulnerability Disclosure

After Solution Corrected

1. CSP shall establish the necessary CVE with the support of the NCCA and related national CSIRT,
2. Proceed to its publication on the relevant list
3. ENISA shall be informed of all changes of status of the related certificates.

NCCA as coordinator

- ✔ NCCAs may develop their capacity to act as "coordinators" as defined in ISO/IEC 29147, and alternatively, designate their national CSIRT to play this role.

  CSIRT shall have access to the necessary details related to the vulnerabilities and to the certified cloud services.

Embargo, notification, and public disclosure guidelines for vulnerabilities found in certified solutions.

Vulnerability Management

EUCC VS EUCS

It is important to understand that the vulnerability handling requirements defined here are related to the maintenance of the certificate more than to the handling of vulnerabilities itself. In particular, the timelines indicated are not realistic for the handling of vulnerabilities, but only for the exchanges with the CAB. They are mostly interesting for complex and impactful vulnerabilities (e.g., Log4J), which take a long time to fully analyse and address.

EUCS is strongly inspired from EUCC

Few significant simplifications (e.g. no mention of an attack potential in the analysis of a vulnerability)

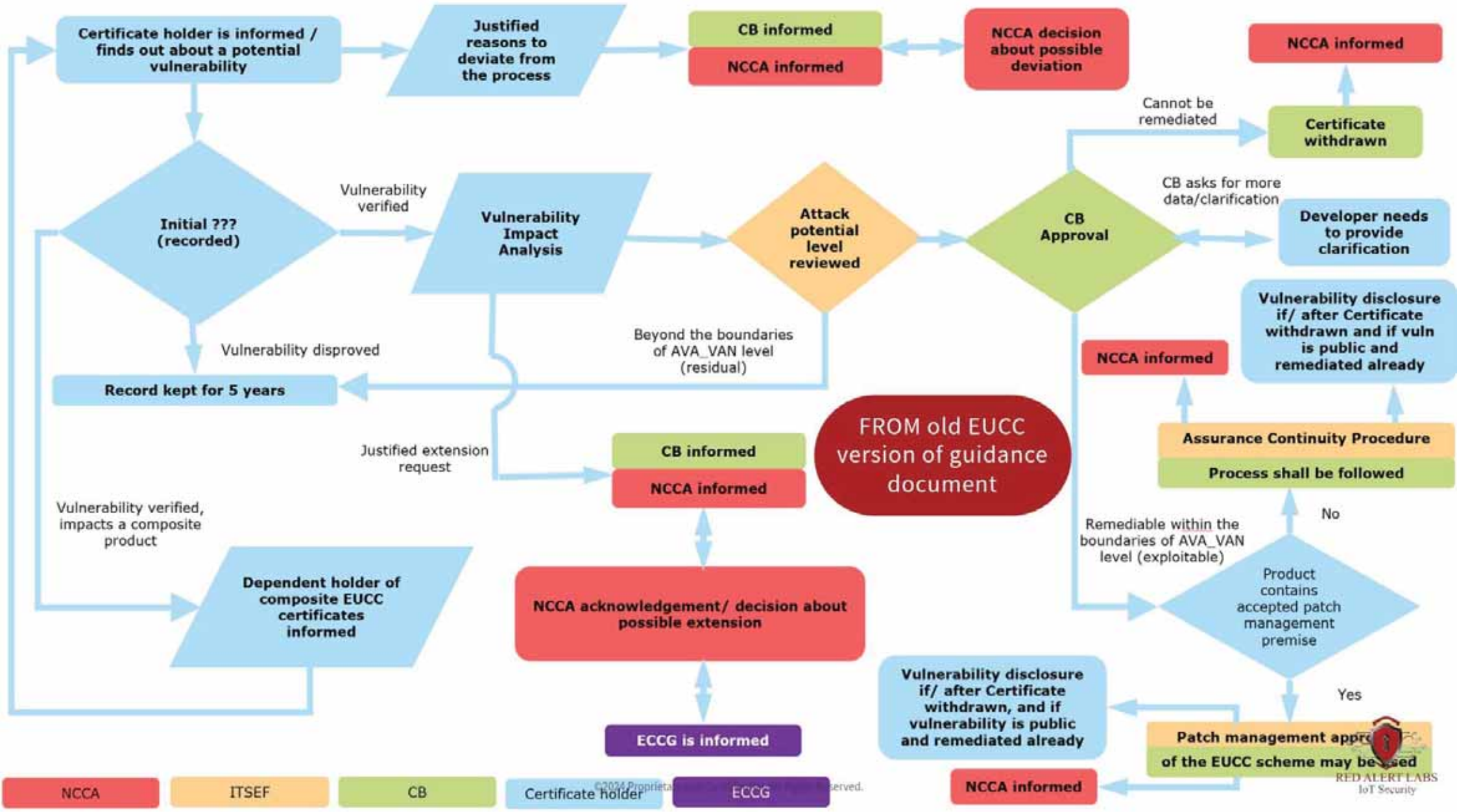
Decision about the suspension and the need to perform another conformity assessment

Is only expected when an incident is linked to a dysfunction in the application of processes

Timelines indicated are limits

- vulnerabilities are expected to be handled timely
- Initial analysis is limited to 90 days
- should normally be under 15 days.

RED ALERT LABS
IoT Security


Certificate holder is informed / finds out about a potential vulnerability
Justified reasons to deviate from the process
CB informed
NCCA informed
NCCA decision about possible deviation
NCCA informed
Cannot be remediated
Certificate withdrawn
Initial ??? (recorded)
Vulnerability verified
Vulnerability Impact Analysis
Attack potential level reviewed
CB Approval
CB asks for more data/clarification
Developer needs to provide clarification
Vulnerability disproved
Record kept for 5 years
Beyond the boundaries of AVA_VAN level (residual)
Vulnerability disclosure if/ after Certificate withdrawn and if vuln is public and remediated already
NCCA informed
Assurance Continuity Procedure
Process shall be followed
Justified extension request
CB informed
NCCA informed
FROM old EUCC version of guidance document
Vulnerability verified, impacts a composite product
Dependent holder of composite EUCC certificates informed
NCCA acknowledgement/ decision about possible extension
Remediable within the boundaries of AVA_VAN level (exploitable)
No
Product contains accepted patch management premise
Yes
Vulnerability disclosure if/ after Certificate withdrawn, and if vulnerability is public and remediated already
Patch management appro
of the EUCC scheme may be used
ECCG is informed
NCCA informed
NCCA
ITSEF
CB
Certificate holder
ECCG
RED ALERT LABS
IoT Security

Question time

- **Question #1**
  What are the 6 steps of vulnerability management?
- **Question #2**
  What is the default limit for the embargo period in the case of the EUCS?
- **Question #3**
  True or False. CSIRT shall act as coordinator during the vulnerability disclosure process.

RED ALERT LABS
IoT Security

Answer

- 1-What are the 6 steps of vulnerability management?
  - Preparation, receipt, verification, remediation development, release, post release
- 2-What is the default limit for the embargo period in the case of the EUCS?
  - 3 months and could be extended with the approval of the NCCA
- 3-True or False. CSIRT shall act as coordinator during the vulnerability disclosure process.
  - False. NCCAs may develop their capacity to act as “coordinators” as defined in ISO/IEC 29147, and alternatively, designate their national CSIRT to play this rol

RED ALERT LABS
IoT Security

Chapter 15 + 18

Record retention + Availability of information

EUCS - Chapter 15 + 18

Record retention

Maintain a records system

according to ISO/IEC 17065

Exhaustive

- shall include all records and other documents produced in connection with each conformity assessment
- Shall allow reproductubility of the evaluation

Robust

stored for a period of at least seven (7) years after the conformity assessment

+

at least five (5) years after the expiry or withdrawal of the certificate

Split responsibility

between the CAB and the CSP regarding the documents and evidence that the CSP made available in a restricted manner to the CAB

RED ALERT LABS
IoT Security

Chapter 16

Related scheme

EUCS - Chapter 16

Related scheme

1/ SecNumCloud

ANSSI

2/ C5 methodology

BSI

3/ Zeker-Online

Zeker-Online foundation

RED ALERT LABS
IoT Security

EUCS - Chapter 16

Related scheme

1 | What happens if I own a certificate of this type?

A certificate issued under these schemes may where necessary be transformed into a certificate under the EUCS scheme if all required activities are conducted.

2 | Is results from evaluations under these schemes can be reused?

A CAB **may accept** to use the results of evaluation activities performed under these schemes for a certification under the EUCS scheme.

3 | Can I continue to be accredited according to these schemes?

EU Member States may consider to establish a date of two (2) years after the implementing act has been adopted for existing schemes to cease producing effect.

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

FAQs

RED ALERT LABS
IoT Security

Chapter 17

Certificate Format

EUCS - Chapter 17

Certificate format

A unique identifier established by the CAB and following ENISA specification

Information related to cloud service and CSP

- Name of the cloud service
- Version of the cloud service
- Name and contact of the CSP
- Link to CSP Website

Information related to evaluation / certification

- Name of the CAB (issuer)
- Name of the CAB (tester)
- CAB(s) Contacts
- Name of the NCCA
- Reference to EUCS
- Reference to the certification report
- EUCSA assurance level
- EUCS assurance level
- Reference to CSEP(s)
- Date of issuance and valitidy period

RED ALERT LABS
IoT Security

Chapter 18

Availability of information

(See with Chapter 15)

Chapter 19

Certificate Validity

EUCS - Chapter 19

Certificate validity

3

Maximum 3 years

Can be less

if the CAB believes that issuing a certificate for three (3) years would lead to potential risks.

RED ALERT LABS
IoT Security

Chapter 20

Disclosure policy

EUCS - Chapter 20

Disclosure policy

Who shall publish the certificate, amendments and withdrawals ?

ENISA

On a dedicated website

Issuing CAB

On its website with a Link to ENISA website

NCCA

On its website with a Link to ENISA website

(CSP)

On its website with a Link to ENISA website

Not mandatory for CSP

RED ALERT LABS
IoT Security

Question time

- **Question #1**
  What is the minimum retention period of the record after the conformity assessment?
- **Question #2**
  What is the minimum retention period of the record after the certificate expiration?
- **Question #3**
  What is the maximum certificate validity?

RED ALERT LABS
IoT Security

Answer

- What is the minimum retention period of the record after the conformity assessment?
  - 7 years
- What is the minimum retention period of the record after the certificate expiration?
  - 5 years
- What is the maximum certificate validity?
  - maximum 3 years and could be less if the CABs judge that there is a risk

RED ALERT LABS
IoT Security

Chapter 21

Mutual recognition

EUCS - Chapter 21

Mutual recongition

- Supported and inspired from the EUCC
- 17 Conditions listed for recognition of certificates by participants to such an MRA, i.e :
  - Accept any participant
  - Use commonly accepted ICT security evaluation
  - Use equivalent evaluation criteria that those listed in EUCS
- CAB(s) of the participants of such an Agreement that issue(s) certificates at an assurance level equivalent to ‘high’ shall be subject to peer assessments

  The procedure may be adapted and simplified for the assurance levels 'basic' or 'substantial'

RED ALERT LABS
IoT Security

Chapter 22

Peer assessment

EUCS - Chapter 22

Peer assessment

Peer review

- Defined by EUCSA (Art. 59)
- Between NCCA

VS

Peer Assessment

- Defined by EUCS
- Between CAB
- Only for CAB issuing CS-"High"

EUCS - Chapter 22

Peer assessment

Shall be based on the rules defined for EUCC

Target

Each authority or body issuing certificates at the evaluation levels CS-High

Period

Every 5 years Maximum

Actors

ECCG --> Establish and maintain planning

CAB --> Perform the assessment

NCCA --> a representative of the NCCA of the assessed CAB participate

ENISA --> May participate

Goals

- assess that they work in a harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composition,
- identify any potential strength that result out of their daily work and that may benefit to others;
- identify any potential weakness that result out of their daily work;
- find a harmonised way to handle nonconformities and vulnerabilities and exchange best practices regarding the handling of complaints.

Result

peer assessment report, with an indication of the severity of any shortcomings

RED ALERT LABS
IoT Security

EUCS - Chapter 22

Peer assessment

Procedure overview

Review of the CAB documentation.

document findings in a peer assessment report delivered to the ECCG.

1-Preparation → 2-Site visit → 3-Reporting → 4-Adoption of report

≃ two-week visit to assess the CAB's technical competence and monitor current evaluation activities.

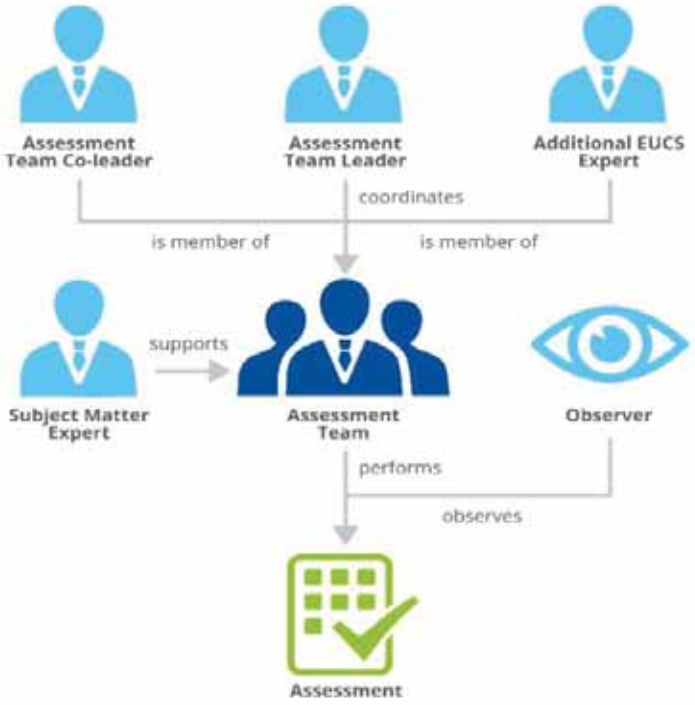
conclude with the adoption of an opinion.

RED ALERT LABS
IoT Security

EUCS - Chapter 22

Peer assessment

Responsibilities sharing



Primary assessment team

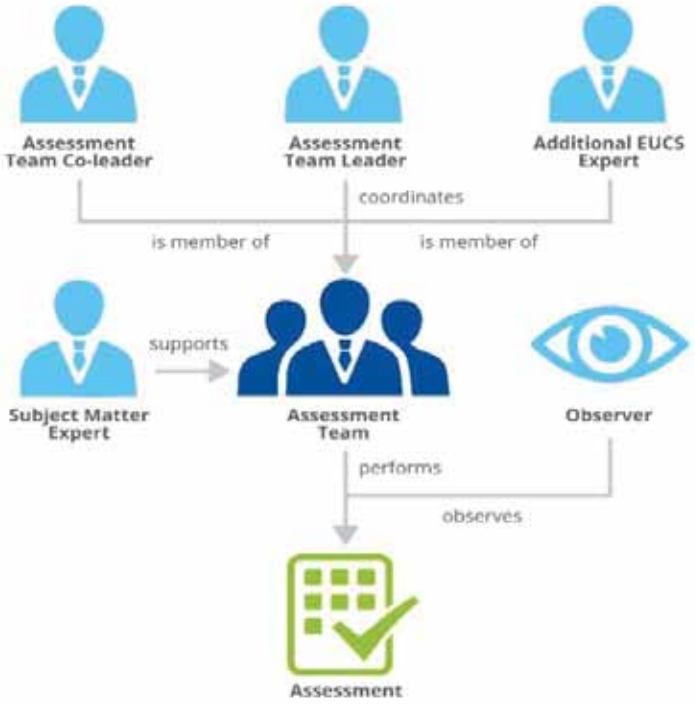
- is composed by the ECCG
- shall be composed of two EUCS experts (Leader and co-Leader) selecting from two CABs issuing certificate (CS-High)
- may be extended with additional EUCS experts from other or the same CABs
- an expert from the concerned NCCA may be associated to the team
- may be assisted by subject matter experts.
- can be observed by observers proposed by other NCCAs

RED ALERT LABS
IoT Security

EUCS - Chapter 22

Peer assessment

Responsibilities sharing



Selected experts shall:

- have a **minimum of two years of experience** as a certifier at a CAB issuing EUCS certificates at evaluation levels CS-high;
- (at least 1 expert) have previously participated to the assessment of additional competences of CABs
- have participated in previous peer assessments under the EUCS scheme (highly recommended)

RED ALERT LABS
IoT Security

EUCS - Chapter 22

Peer assessment

Responsibilities sharing

Peer assessed CAB

- Provide documentation (description of the scope, last certificates issued, procedures for certification, list of personnels with their competences, ...)
- Provide quality management system
- Provide documents in English, at least 4 weeks before audit date
- Provide documents that have been used and produced during the certification of the cloud services assessed during peer assessment.
- Coordinate site visit
- Beeing generally available to answer questions and resolve issues

RED ALERT LABS
IoT Security

EUCS - Chapter 22

Peer assessment

Responsibilities sharing

Peer assessment team leader

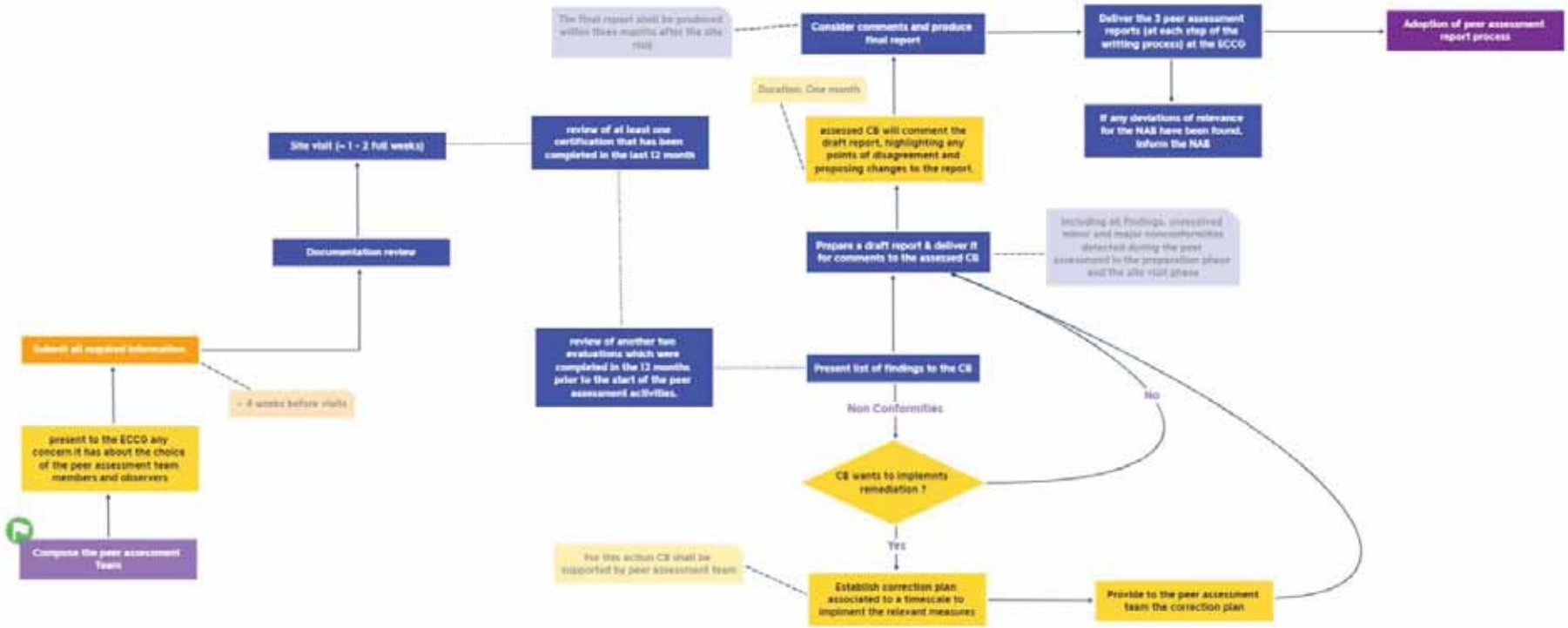
- Coordinating the receipt of materials from the CAB,
- Coordinating the decision regarding the selection of the candidate cloud services (and audit organisations) and notification to the peer assessed CAB,
- Drafting the site visit(s) agenda and coordinating it with the CAB,
- Coordinating and completing the peer assessment draft report at the end of the site visit,
- Delivering the peer assessment final report to the ECCG, and
- If necessary, monitoring the CAB's resolution of outstanding issues resulting from the peer assessment.

RED ALERT LABS
IoT Security

EUCC - Chapter 22

Peer assessment

Process

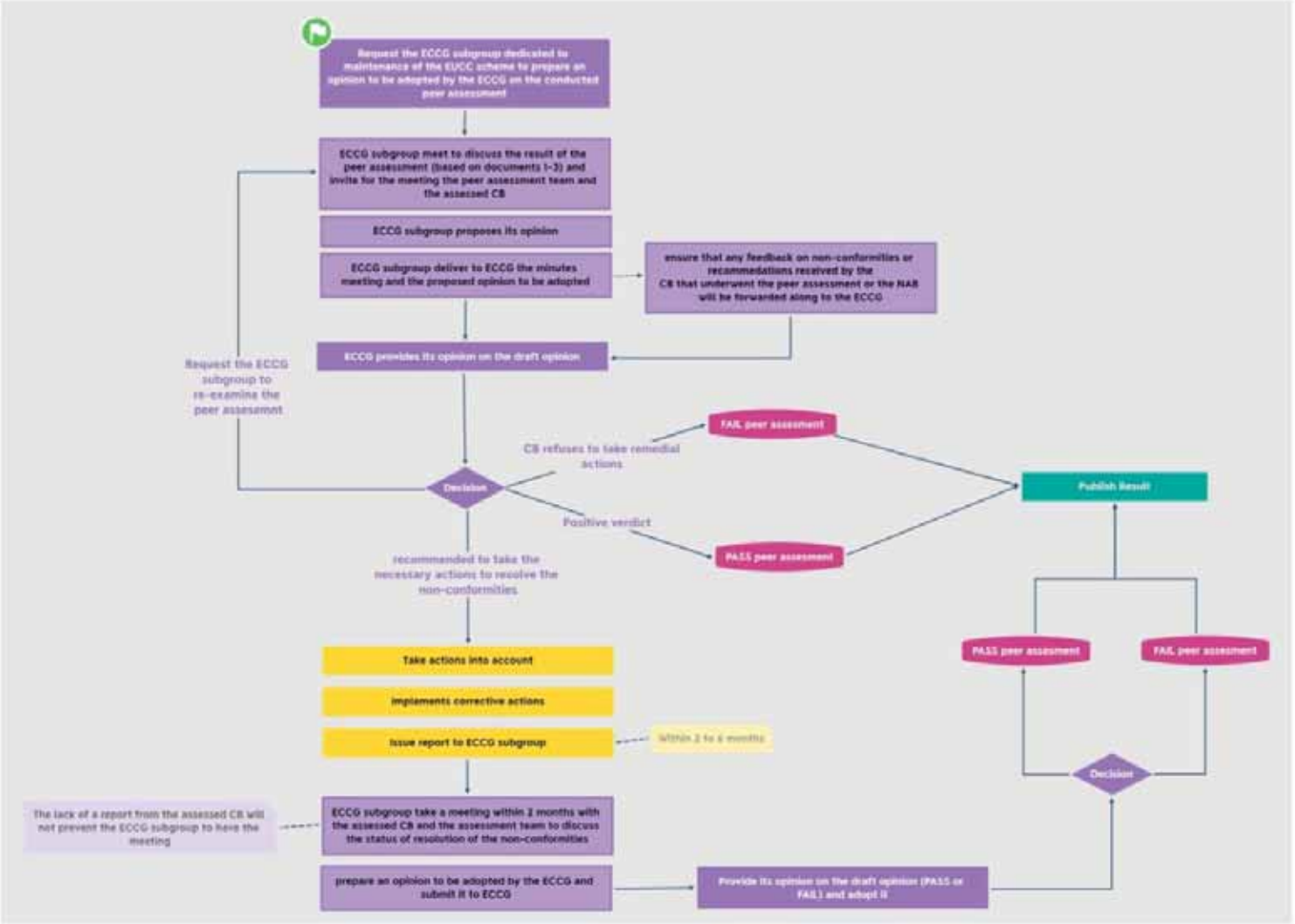


RED ALERT LABS
IoT Security

EUCC - Chapter 22

Peer assessment

ECCG verdict



Chapter 23

Supplementary information

Only a reminder of the EUCSA, requirement already covered in chapter 17 and 12

Chapter 24

Additional topics

EUCS - Chapter 24 - Additional topics

1- Extension profile

CSEP

- The scheme users have the ability to extend the EUCS requirements in the context of a specific use case

  Specific requirement are defined in an EUCS extension profile (CSEP)

- A specific evaluation process has been defined for extension profiles
  1. Developped by a scheme user
  2. Evaluation by CAB
  3. Review by NCCA
  4. Approved By ECCG
  5. Published by ENISA

- A CSEP shall
  - not remove or weaken any requirement defined in the EUCS.
  - not modify the assessment methodology or the assessment methods defined in the EUCS.
  - follow the processes defined in the EUCS, and shall produce the same deliverables.
  - specify the minimum EUCS evaluation level that it targets.
  - define new service requirements (that do not contradict or weaken EUCS requirements).

- Maximum validity period

  5 years

EUCS - Chapter 24 - Additional topics

2- Security of information

2 main information in this chapter

Confidentiality

all parties involved in the application of this scheme shall maintain confidentiality and observe professional secrecy

Use

All information received from the CABs or their subcontractors or the CSPs shall only be used for the purpose of the certification

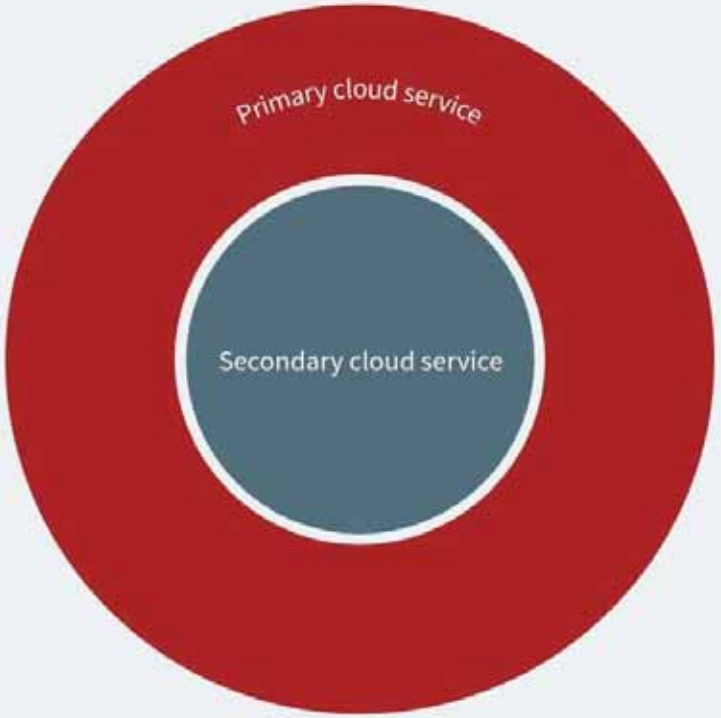
RED ALERT LABS
IoT Security

3- Composition

1 | **A particular case of certification where**
the cloud service to be certified (primary cloud service) uses a subservice that is itself a cloud service (secondary cloud service) that has been certified in the EUCS.

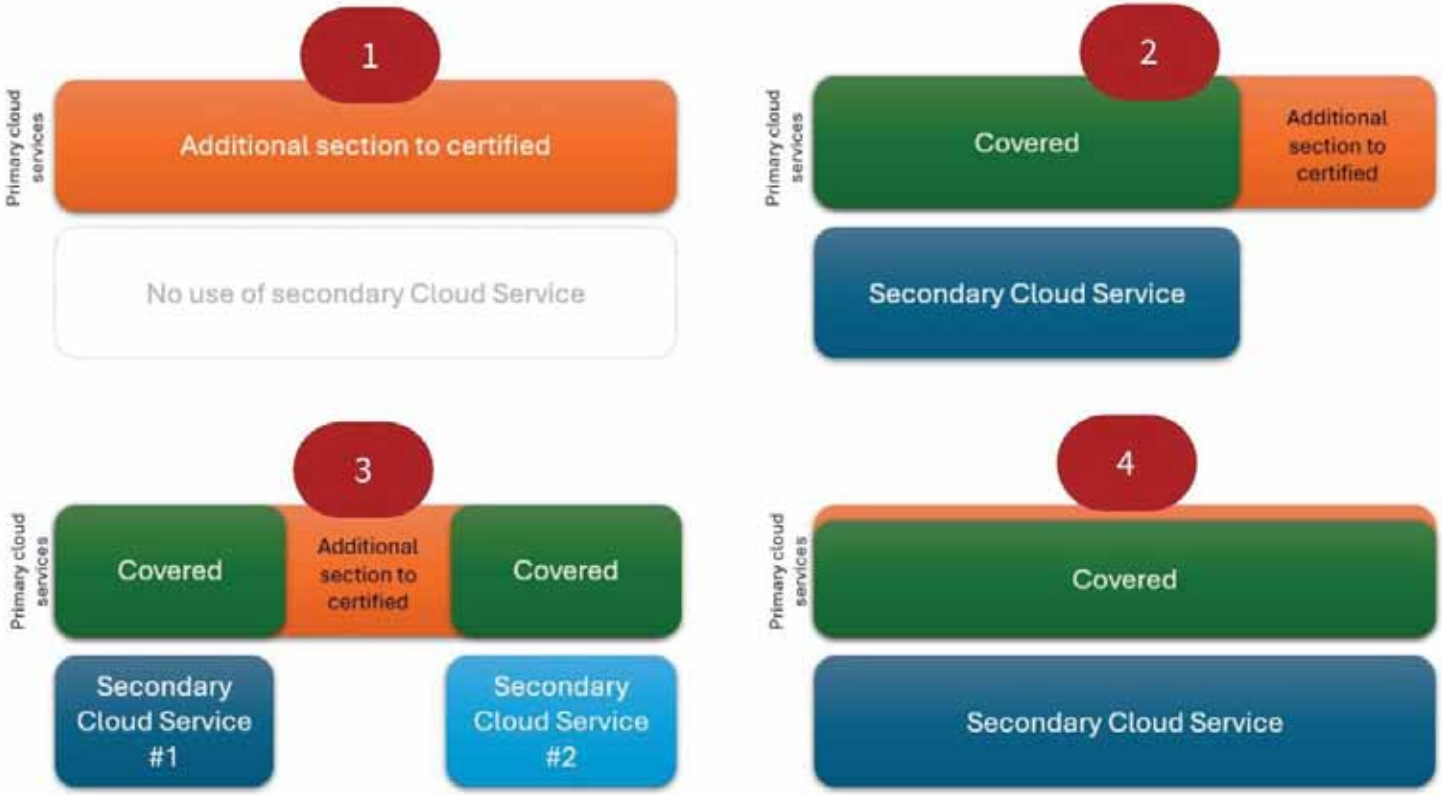
2 | **The secondary cloud service**

- provide a description of the contribution of their cloud service to the EUCS requirement fulfilment of primary cloud services that depend on it, properly justified through references to their own controls.
- provide a list of actionable requirements on Complementary Customer Controls (CUEC), to be fulfilled by a primary cloud service that relies on their service in order for that primary cloud service to fulfil the requirements for EUCS certification at the chosen assurance level



3- Composition

Some example of composition



RED ALERT LABS
IoT Security

Question time

- **Question #1**
  What are the 4 steps related to the peer assessment process?
- **Question #2**
  Could you list 2 requirements related the CSEP?
- **Question #3**
  True or False. In order to apply composition, the secondary cloud service shall be certified at an evaluation level equal or lower than the evaluation level targeted by the primary cloud service;

RED ALERT LABS
IoT Security

Answer

- What are the 4 steps related to the peer assessment process?

  - Preparation, Visit, Reporting, Adoption of Report

- Could you list 2 requirements related the CSEP?

  Below is the full list of requirements:

  * not remove or weaken any requirement defined in the EUCS
  * not modify the assessement methodology or the assessment methods defined in the EUCS
  * follow the processes defined in the EUCS, and shall produce the same deliverables
  * specify the minimum EUCS evaluation level that it targets,
  * define new service requirements (that do not contradict or weaken EUCS requirements).

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

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

RED ALERT LABS
IoT Security

Thank you

RED ALERT LABS
IoT Security

Campus Cyber, 5 Rue Bellini, 92800 Puteaux , France

3 rue Parmentier, 94140, Alfortville, France

https://www.redalertlabs.com

+33 9 51 79 07 87

@RedAlertLabs

/company/red-alert-labs