RED ALERT LABS
IoT Security

# EUROPEAN CLOUD SERVICE SCHEME (EUCS SCHEME)

TRAINING

September 2021

A4CEF

Co-financed by the Connecting Europe Facility of the European Union

# EUCS SCHEME TRAINING – TABLE OF CONTENTS




A4CEF

Co-financed by the Connecting Europe Facility of the European Union

# SELF-ASSESSMENT

# ASSESSMENT METHODOLOGY: SELF-ASSESSMENT

*The issuance of EU statements of conformity by cloud service providers could only have been allowed for all cloud services that present a low risk (Article 53(1)), i.e., to a subset of the cloud services that could be certified at level Basic.*

The ad hoc Working Group consistently expressed that self-assessment was not suitable for cloud services, even at level Basic and even on a strictly defined subset of services. Some of the reasons:

- new elements in the scheme (example: security objectives and requirements)
- Avoid wrong interpretations by CSPs and allow accredited CABs to use the scheme,
- control the usage in the meantime through guidance and guidelines for CABs.

**Decision: not allow the issuance of EU statements of conformity in the initial version of this scheme, as there are enough challenges to be met in that first version.**

**This decision may be reconsidered in future releases of the scheme.**

# SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

# SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

All CABs performing assessments in the context of the EUCS scheme will need to be accredited for [ISO17065].

The requirements will define several profiles corresponding to the various roles in the conformity assessments, in order to allow CABs that only perform a subset of the of the conformity assessment activities, in particular those that only perform evaluation activities.

The technical competence requirements associated to accreditation are sufficient to perform conformity assessments at levels Basic and Substantial. **However**, advanced competences are required in order to perform a conformity assessment at level High.

# SPECIFIC REQUIREMENTS APPLICABLE TO A CAB

As a consequence, conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out in the context of an evaluation at level High conformity assessment tasks related to highly technical topics including:

- *Penetration testing, including the design and performance of penetration tests and the analysis of penetration testing activities performed by a CSP or its contractors.*
- *Analysis of development activities, and in particular the review of the design and implementation of security measures by the CSP.*

**Further details are to come**

# MUTUAL RECOGNITION

# MUTUAL RECOGNITION

The mutual recognition of certification schemes with third countries shall be supported by the establishment of a Mutual Recognition Agreement (MRA) between the participants.

Some conditions are listed in the Chapter 21 of the actual version and shall be fulfilled. Examples:

- 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 this document;
- Others...

# CERTIFICATE VALIDITY & MANAGEMENT

# CERTIFICATE VALIDITY

The maximum period of validity of the certificates shall be three (3) years.

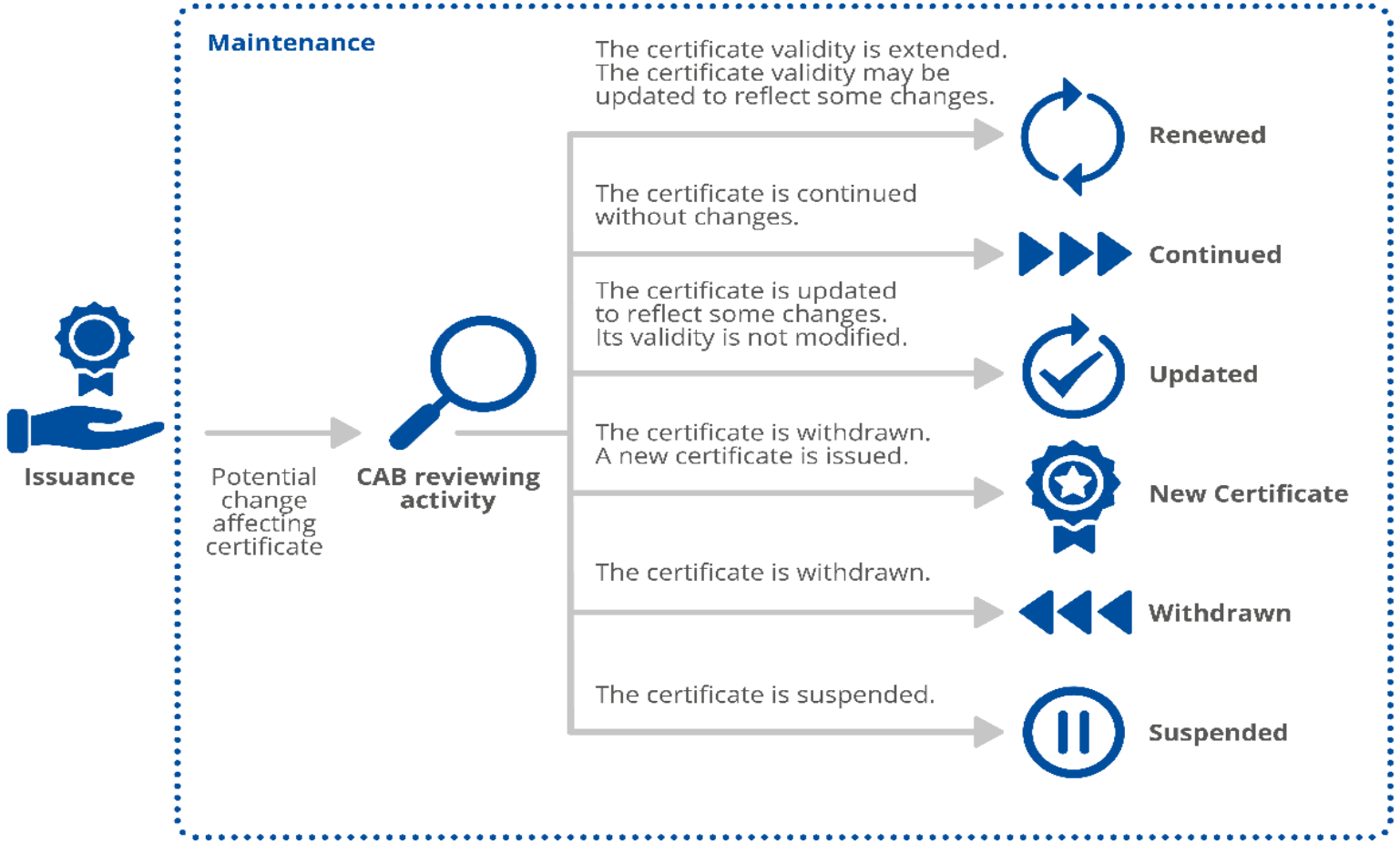
In order to maintain the validity of the certificate for its full period of validity:

- the CSP shall follow the processes defined in in **Chapter 12 (Certificate Management),**
- and the certified cloud service shall be subject to a periodic conformity assessment or to a renewal conformity assessment at most one (1) year after the previous initial, periodic, or renewal conformity assessment.

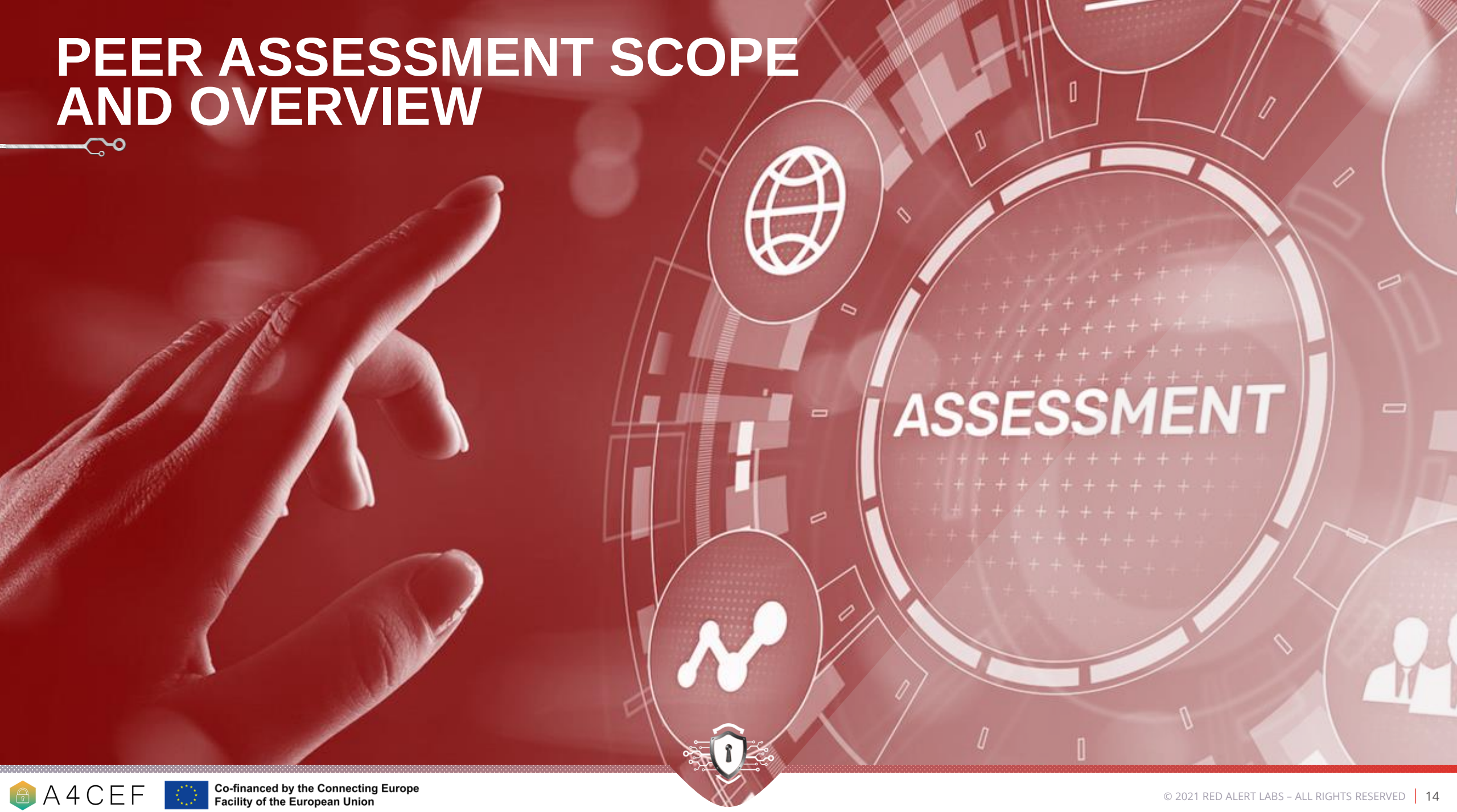
Under certain conditions, and following the processes defined in Chapter 12 (Certificate Management), a CAB may continue a certificate with an extended validity period beyond the initial three (3) years.

- an average maximum of three (3) years was selected for the general case.
- possible to issue a certificate for a shorter period of time, in particular if the CAB believes that issuing a certificate for three (3) years would lead to potential risks.
- The chapter also defines the 1-year limit between periodic assessments. This limit applies to all levels, but the nature of the activities to be performed depends on the level.

# CERTIFICATE MANAGEMENT CHAPTER 12 (CERTIFICATE MANAGEMENT),



# PEER ASSESSMENT SCOPE AND OVERVIEW



# PEER ASSESSMENT

While every authority or body issuing certificates for assurance level ‘high’, including their subcontractors, shall operate under its own responsibility, a peer assessment shall be established for those issuing EUCS certificates at level High to:

- assess that they work in a harmonised way and produce the same quality of certificates;
- allow the reuse of certificates for composite service certification
- identify any potential strength that result out of their daily work
- 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.

**This concerns:**

1. CAB issuing certificates for assurance level ‘high’
2. NCCA

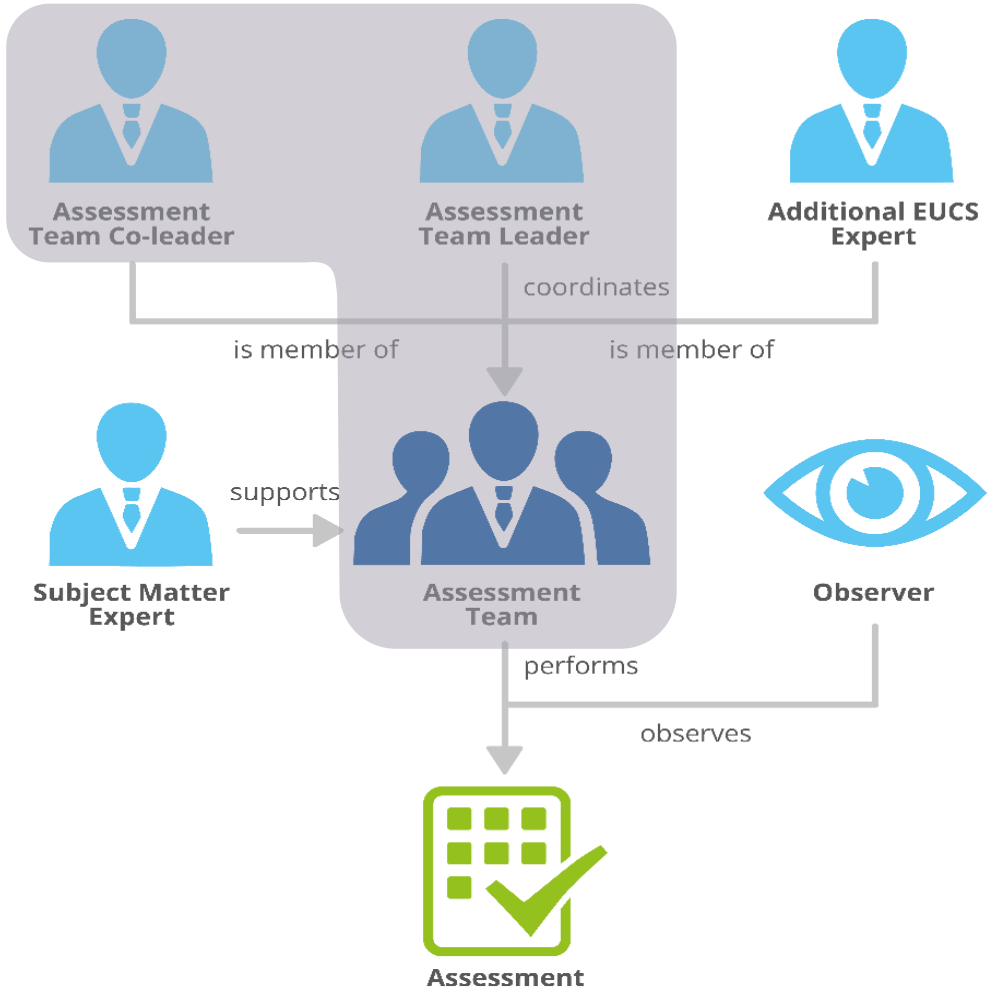
shall take place on a regular basis, with a periodic interval that shall not exceed five (5) years.

# PEER ASSESSMENT: SCOPE

**The procedure consists of 4 phases: preparation, site visit, reporting, and adoption of a report.**

The procedure only defines the process to be followed. In order to be as comprehensive and objective as possible, checklists shall be further developed in cooperation with the ECCG to assist the peer assessment team. These checklists will contain a common understanding of state of the art and operating practices.

# PEER ASSESSMENT: OVERVIEW




The primary assessment team shall consist of:

- two EUCS experts (Leader and co-Leader) selected from two CABs issuing certificates at the assurance level High of the EUCS.
- This primary assessment team may be extended with additional EUCS experts from other or the same CABs, and in the case of a delegation of the issuance of certificates or of prior approval of certificates, an expert from the concerned NCCA may be associated to the selected CAB expert into the team.

# PEER ASSESSMENT: OVERVIEW

- The peer assessment team may be assisted by subject matter experts.
- The peer assessment may be observed by observers proposed by other NCCAs.
- The peer assessed CAB may present to the ECCG any concern it has about the choice of the peer assessment team members and observers, for example in case of a conflict of interest

# PEER ASSESSMENT: OVERVIEW

## Preparation

- involve the review of the CAB documentation by the members of the peer assessment team
- become familiar with the CAB's policies and procedures.

## Site Visit

-consist of a two-week visit by the peer assessment team to the CAB

- assess the CAB's technical competence, and where applicable of auditors performing evaluation activities.

-exact duration of site visit depends on the possible reuse of existing peer assessment evidence and results, and on the number of auditors subcontracted by the CAB.

## Reporting

- assessment team will document their findings in a peer assessment report delivered to the ECCG.

## Adoption

- adoption of an opinion by the ECCG of the outcome of the peer assessment.

# QUIZ

- Is self assessment authorized?
- Complete the sentence. All CABs performing assessments in the context of the EUCS scheme will need to be accredited for [ISO170??]
- True or False. Conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out in the context of an evaluation at level Substantial conformity assessment tasks.
- What is the maximum period of validity of the certificates?

# QUIZ

- Is self assessment authorized?

Yes and No ☺. Self-Assessment could be done for Basic level by the CSP but the results should be audited by a CAB

- Complete the sentence. All CABs performing assessments in the context of the EUCS scheme will need to be accredited for [ISO170??]

17065.

- True or False. Conformity assessment bodies shall be authorised by the national cybersecurity certification authority to carry out in the context of an evaluation at level ~~Substantial~~ HIGH conformity assessment tasks.

False.

- What is the maximum period of validity of the certificates?

The maximum period of validity of the certificates shall be three (3) years.

# COMPLIANCE MONITORING

# COMPLIANCE MONITORING

**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.**

## General cases of non-compliance:

a non-compliance in the application by a CSP of the rules and obligations related to a certificate issued on their cloud services;

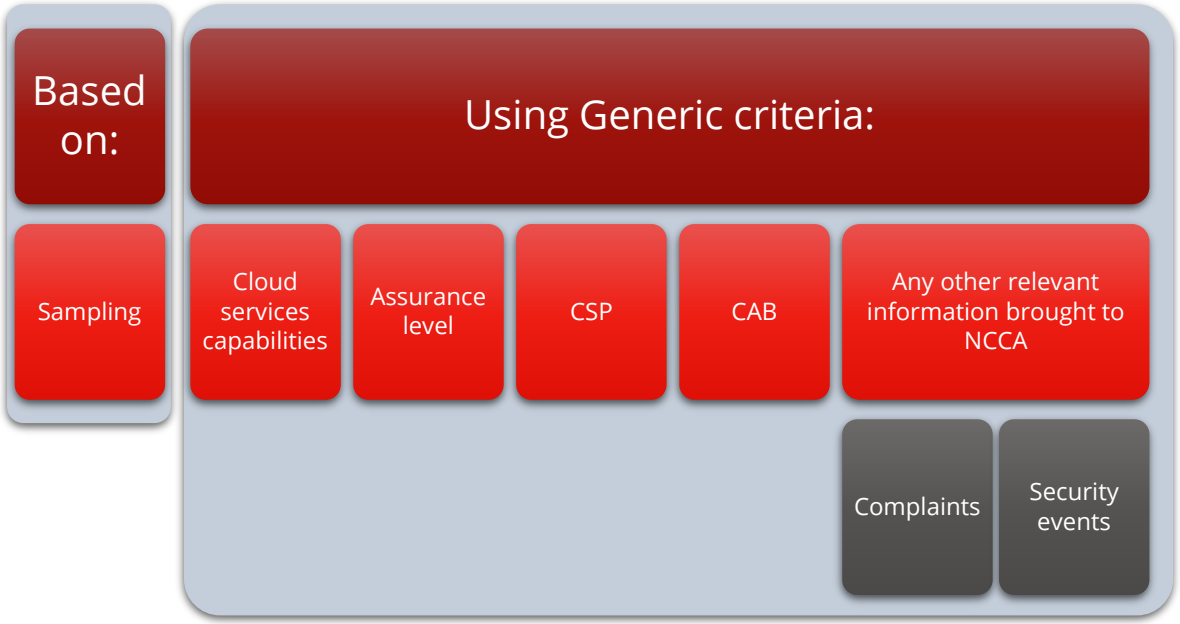
a non-compliance in the conditions under which the certification takes place and that are not related to the individual cloud service;

a nonconformity of a certified cloud service with the EUCS security requirements, which includes and is not limited to:

- a change in the cloud service itself leading to a change of the cloud service's security posture;
- a significant security incident that has affected the certified cloud service or has resulted in a data breach or loss of sensitive information;
- a change in the threat environment after the issuance of the certificate, which has an adverse impact on the security of the certified cloud service;
- a vulnerability identified and related to the certified cloud service, that has an adverse impact on the security of the certified cloud service.

# COMPLIANCE MONITORING: NCCA ROLE

## THE GENERAL MONITORING OF THE CERTIFIED CLOUD SERVICES SHALL BE:





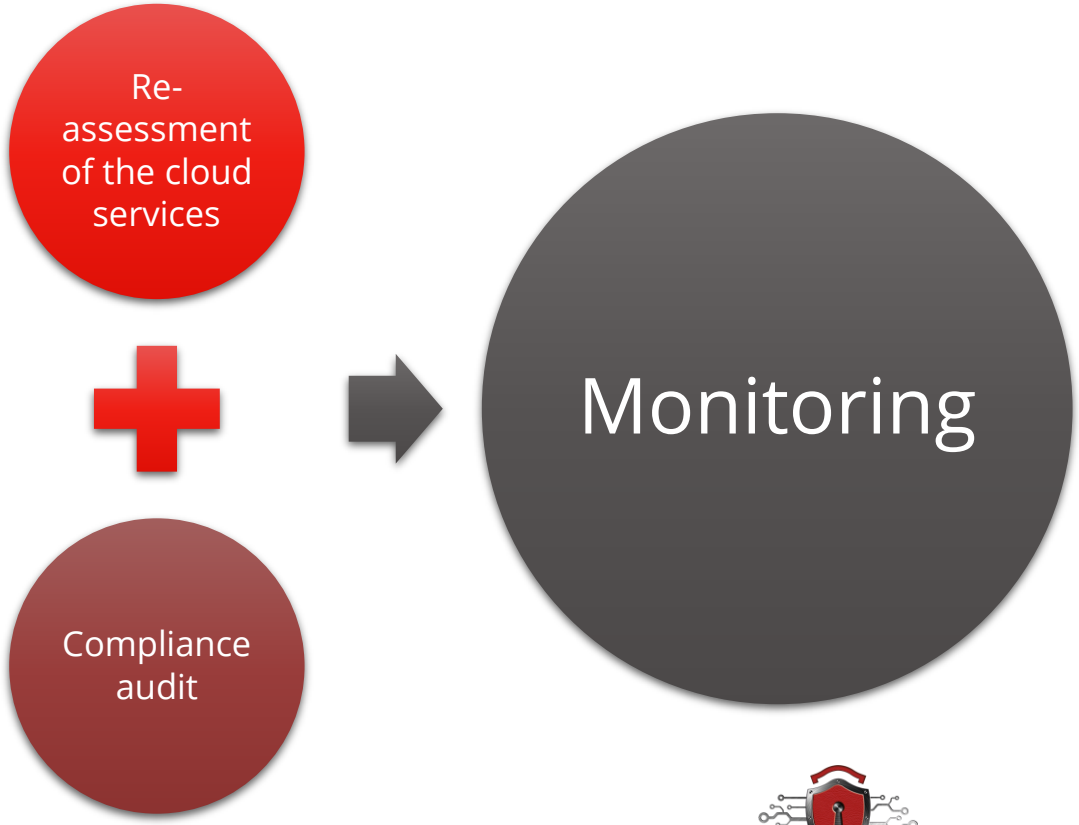

Sample annually a minimum of 5% of the cloud services which have been the subject of a successful conformity assessment in the context of the EUCS scheme in the previous year



and at least one cloud service per annum.

# COMPLIANCE MONITORING: NCCA ROLE

NCCA shall involve in the monitoring the CAB that has issued the certificate, and if necessary, its subcontractors




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

# COMPLIANCE MONITORING: NCCA ROLE

Re-assessment of the cloud services

## In the first step of the re-assessment,

- the NCCA shall perform again the review phase performed by the CAB before taking the decision to issue or maintain the certificate, based on the documentation that was available at the time to the reviewer.
  - **IF NEEDED FOR THEIR REVIEW, THE NCCA MAY CONTACT THE CSP IN ORDER TO BE GRANTED ACCESS TO THE DOCUMENTS FOR WHICH THEY HAVE ONLY PROVIDED RESTRICTED ACCESS TO THE CAB DURING THE AUDIT.**
- Following this review, the NCCA may request additional information about any of the activities performed during any stage of the conformity assessment. For each activity, the NCCA may:

request additional information and explanations from the CAB;

have the CAB perform the activity again, possibly while monitored by a NCCA representative;

have a NCCA representative perform the activity again.

# COMPLIANCE MONITORING: NCCA ROLE

Compliance audit

- The NCCA may request a compliance audit if they have some reasons to doubt that a CSP complies to all their obligations with respect to the scheme, for instance after receiving a complaint.

- The NCCA shall address a compliance audit request to the CAB, indicating the potential non-compliance that is suspected. Then, the process should be as follows:

The CAB shall transmit the request to the CSP, after adding any information that they deem suitable based on their knowledge of the certified cloud service;

The CSP shall then analyse the request and provide a motivated answer to the CAB, describing in particular any non-compliance or nonconformity they may have detected in their analysis, accompanied by supporting documentation if required;

The CAB shall then analyse the answer from the CSP, and transmit the CSP's answer with their analysis back to the NCCA.

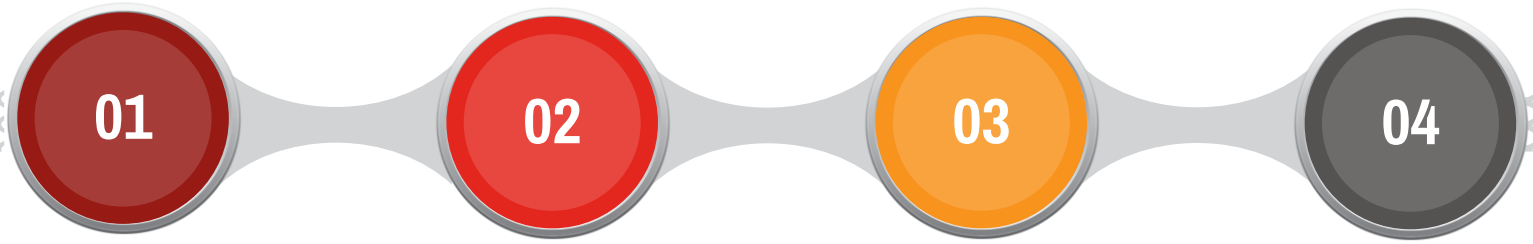
# COMPLIANCE MONITORING: NCCA ROLE

The following deviations and irregularities shall be considered as potential non-compliance elements in the application by a CSP of the rules and obligations related to a certificate issued on their cloud service:

- any deviation from the requirements applicable to the information supplied or made available to CAB, discovered after the emission of a certificate (ex: version of the information, self-established evidence, …)
- any deviation from the requirements regarding the certificate content and the supplementary information (ex: proper cloud service identifier, cloud service scope, …)
- any deviation from the requirements on the certificate holder's obligations towards maintaining the certificate validity.(ex: failure to apply mandatory maintenance activities, failure to implement and enforce mandatory processes as requested by terms and conditions, …)

# COMPLIANCE MONITORING: NCCA ROLE

**SUCH NON-COMPLIANCE IN THE APPLICATION BY A CSP OF THE REQUIREMENTS RELATED TO A CERTIFICATE ISSUED ON THEIR CLOUD SERVICE SHALL BE MONITORED BY:**




01 Requiring any applicant to a certificate to commit to the CAB to a number of obligations

02 Using the available dispositive to track the non-respect of the previous obligations

03 An assessment of the gravity of the irregularity by the CAB

04 Using the possibility of the dialog between the CAB and the CSP to try and solve minor issues, and of the provisions of Chapter 13 (Non-Compliance) where necessary

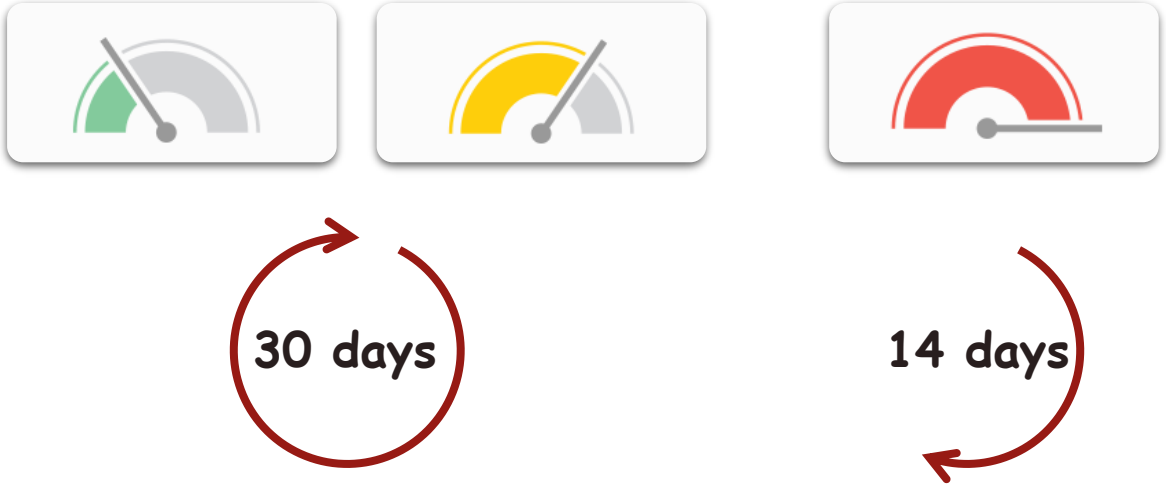
**THE NCCA**

- shall be informed of the results of these activities.
- may establish rules for a periodic dialog between the issuers of certificates and the certificates owners, as to formally check and report the respect of previously stated obligations.

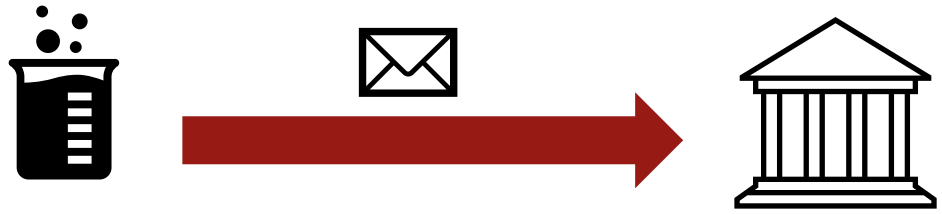
# NON-COMPLIANCE

# NON-COMPLIANCE: CONFIRMED DEVIATION

**CAB who has issued the certificate** shall **request the CSP for assertions and amendments to restore compliance**, to be provided within the **time frame**

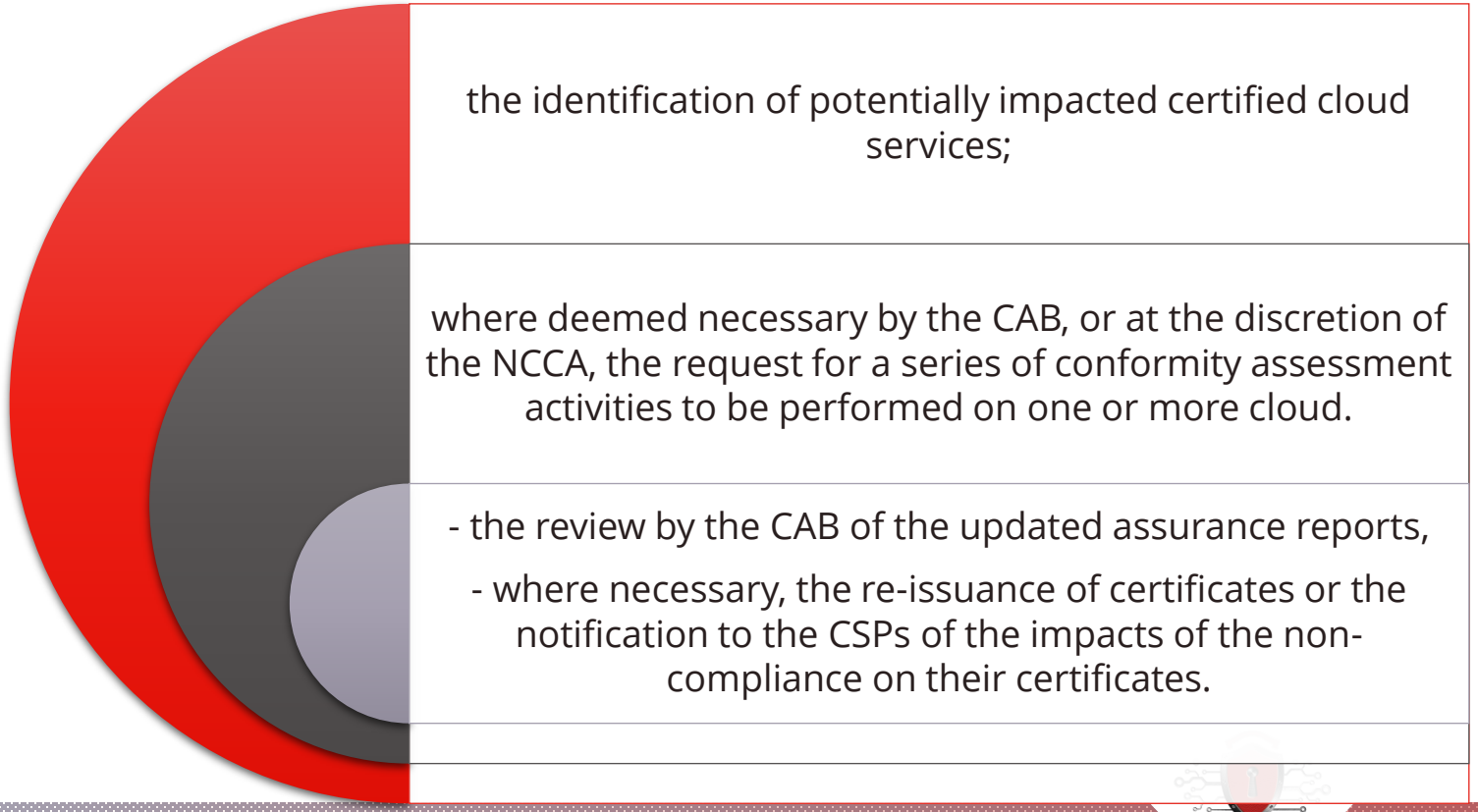



**Continued non-compliance past the allowed time frame** shall trigger a **suspension of the certificate** for the cloud service, a suspension of all certification activities by the CAB on behalf of the CSP for other services, **with information about the suspension by the CAB to the NCCA.**



# NON-COMPLIANCE: CONFIRMED DEVIATION

For a confirmed non-compliance in the conditions under which the certification takes place and that are not related to the individual cloud service, the concerned CAB shall proceed, under the control of the NCCA, to the following:




These activities shall occur within the maximum period (14 or 30 days), which may only be extended after approval by the NCCA.

# QUIZ

- **True or False? The general monitoring of the certified cloud services shall be based on sampling, using generic criteria**
- True or False? Re-assessments and audits shall not be financially supported by the CSP
- True or False? Deviations and irregularities shall be considered as potential non-compliance elements in the application by a CSP of the rules and obligations related to a certificate issued on their cloud service

# QUIZ

- True or False? The general monitoring of the certified cloud services shall be based on sampling, using generic criteria

True

- True or False? Re-assessments and audits shall ~~not~~ be financially supported by the CSP

False

- True or False? Deviations and irregularities shall be considered as potential non-compliance elements in the application by a CSP of the rules and obligations related to a certificate issued on their cloud service

True

# SECURITY CONTROLS

# CATEGORIES OF SECURITY CONTROL

**20 categories**

**120 Security Controls**

| | | | | |
|---|---|---|---|---|
| 4 Organisation of information security (OIS) | 3 Information security policies (ISP) | 3 Risk Management (RM) | 6 Human Resource (HR) | 5 Asset Management (AM) |
| 5 Physical Security (PS) | 22 Operational Security (OPS) | 9 Identity, Authentication & Access control management (IAM) | 4 Cryptography and Key Management (CKM) | 9 Communication Security (CS) |
| 3 Portability and Interoperability (PI) | 6 Change and configuration management (CCM) | 7 Development and information systems (DEV) | 5 Procurement management (PM) | 7 Incident management (IM) |
| 4 Business continuity (BC) | 4 Compliance (CO) | 6 User Documentation (DOC) | 3 Dealing With Investigation Requests From Government Agencies (INQ) | 5 Product Safety And Security (PSS) |

# TOTAL OF **REQUIREMENTS**

| | CS-Basic | CS-Substantial | CS-High |
|---|---|---|---|
| **TOTAL** | **217** | **336** | **414** |
| Organization of information security | 6 | 7 | 8 |
| Information security policies | 10 | 13 | 15 |
| Risk management | 10 | 11 | 12 |
| Human resources | 15 | 21 | 22 |
| Asset management | 9 | 11 | 15 |
| Physical security | 12 | 18 | 24 |
| Operational security | 32 | 47 | 64 |
| Identity, authentication, access control | 21 | 47 | 54 |
| Cryptography and key management | 5 | 10 | 11 |
| Communication security | 15 | 21 | 26 |
| Portability and interoperability | 8 | 11 | 13 |
| Change and configuration management | 8 | 11 | 18 |
| Development | 11 | 23 | 28 |
| Procurement | 12 | 13 | 18 |
| Incident management | 14 | 20 | 24 |
| Business continuity | 3 | 9 | 10 |
| Compliance | 5 | 10 | 15 |
| User documentation | 11 | 14 | 15 |
| Investigation requests | 5 | 6 | 7 |
| Product safety and security | 5 | 13 | 15 |

# ZOOM ON CATEGORIES OF SECURITY CONTROL

## Information Security Policies (ISP)

### ISP-01 Global Information Security Policy

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

### ISP-02 Security Policies And Procedures

Objective: Policies and procedures are derived from the information security policy, documented according to a uniform structure, communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner.

### ISP-03 Exceptions

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

## Identity, Authentication and Access Control Management (IAM)

### IAM-01 Policies For Access Control To Information

Objective: Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.

### IAM-02 Management Of User Accounts

Objective: Policies and procedures for managing the different types of user accounts are documented, communicated and made available in order to ensure that that all accesses to information have been duly authorized.

### ...

### IAM-09 General Access Restrictions

Objective: The assets in and around the cloud service are managed in a way that ensure that access restrictions are enforced between different categories of assets.

# ZOOM ON SECURITY CONTROL - EXAMPLE ISP-02

**Basic**

- The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including at least the following aspects:
  - Objectives;
  - Scope;
  - Roles and responsibilities within the organization;
  - Roles and dependencies on other organisations (especially cloud customers
  - and subservice organisations);
  - Steps for the execution of the security strategy; and
  - Applicable legal and regulatory requirements.
- The CSP shall communicate and make available the policies and procedures to all internal and external employees.
- The CSP's top management shall approve the security policies and procedures or delegate this responsibility to authorized bodies.
- The CSP's subject matter experts shall review the policies and procedures for adequacy at least annually, when the global information security policy is updated, and when major changes may affect the security of the cloud service.
- After an update of procedures and policies, they shall be approved before they become effective, and then communicated and made available to internal and external employees.

**Substantial**

- Basic requirements
- The CSP shall derive policies and procedures from the global information security policy for all relevant subject matters, documented according to a uniform structure, including at least the following aspects:
  - Roles and responsibilities within the organization, including staff qualification requirements and the establishment of substitution rules;
- In case of a delegation, the authorized bodies shall report at least annually to the top management on the security policies and their implementation

**High**

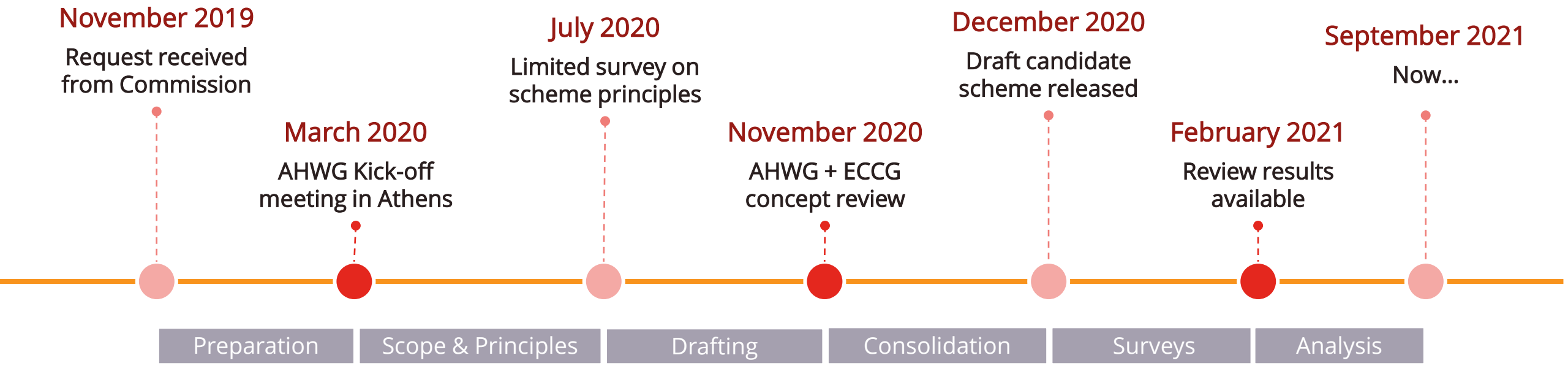
- Similar to substantial


04

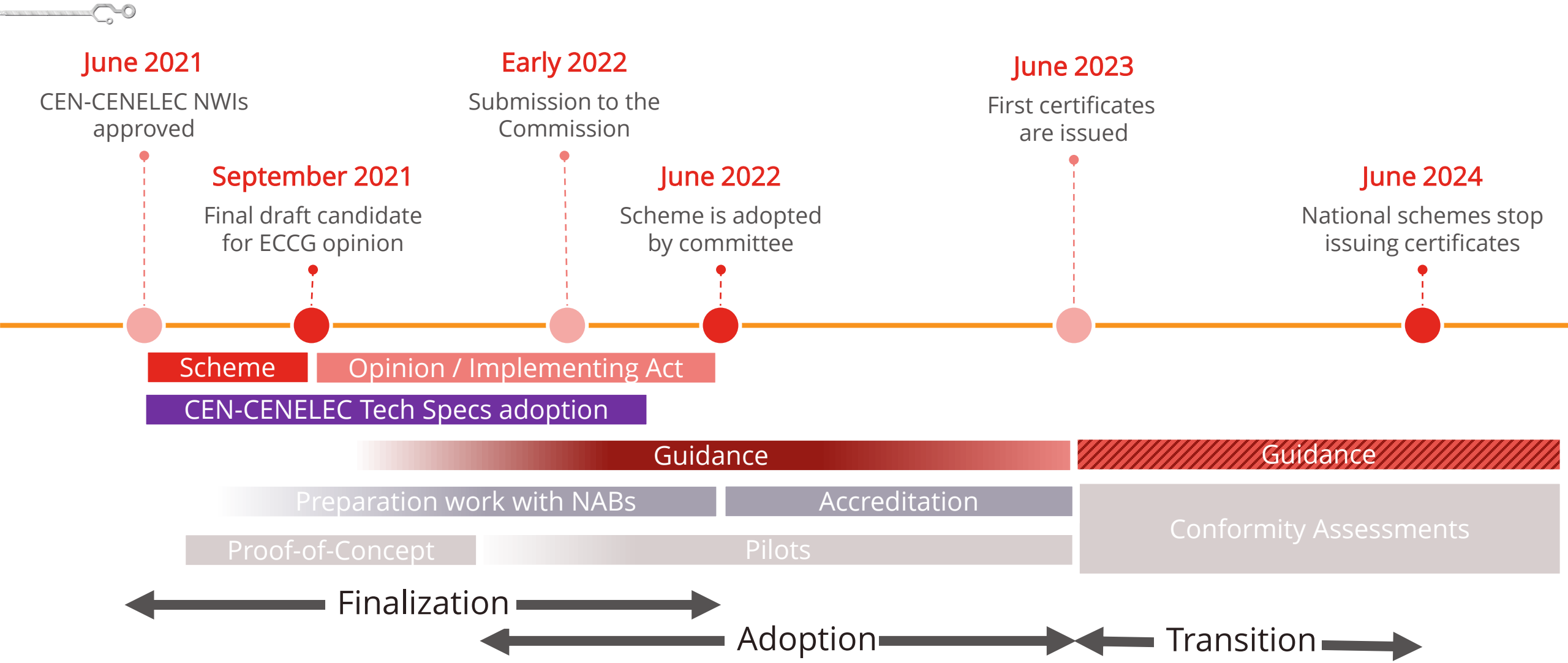
# OVERVIEW OF THE NEXT PHASE

- EUCS TIMING and next steps
- CEN-CENELEC Collaboration
- EUCS ongoing work
- PoC on specific requirements
- Guidance
- Penetration testing

# WHERE IT COMES FROM? (REMINDER)

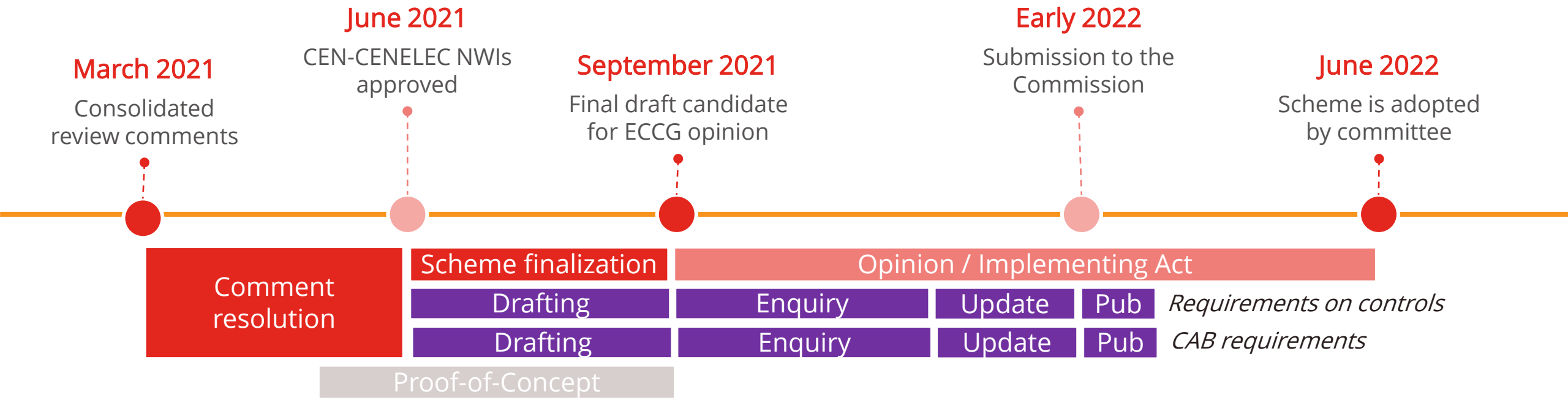


# HIGH LEVEL PLANNING



# FOCUS ON SCHEME FINALIZATION (TENTATIVE)

**THE "CORE" SCHEME AND THE TWO TECHNICAL SPECIFICATIONS WILL FOLLOW PARALLEL PATHS.**

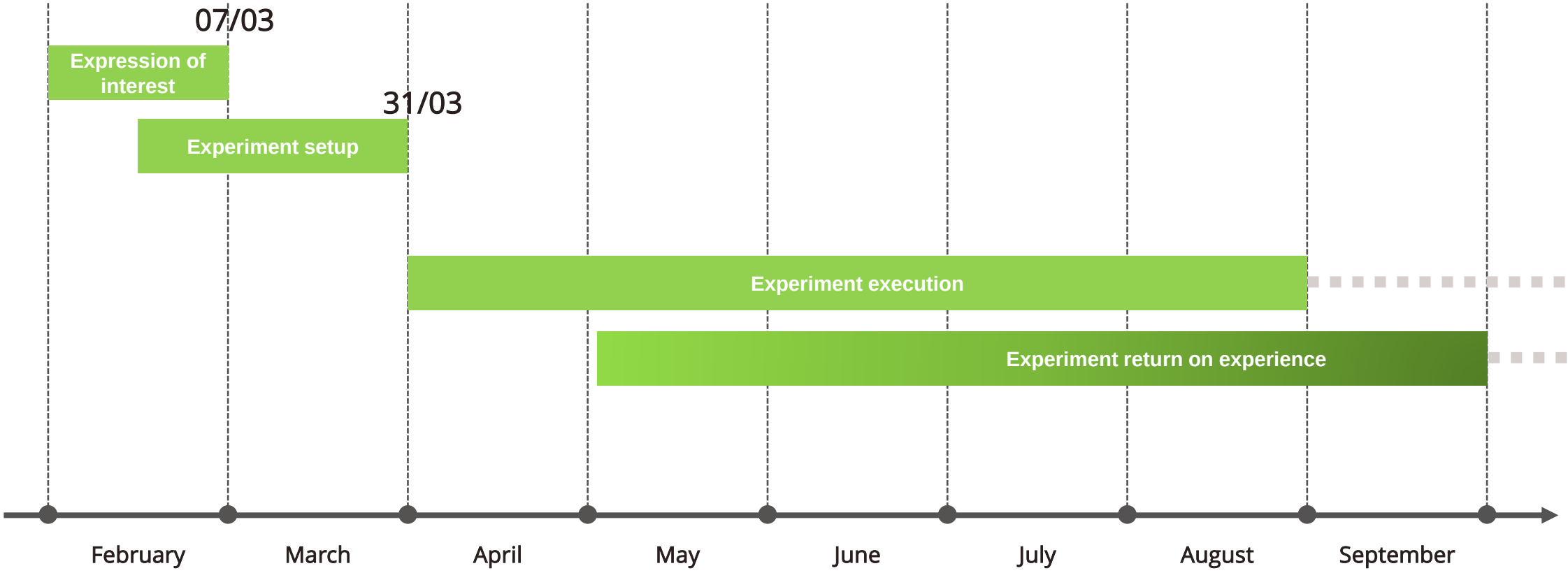



**THE PRESSURE REMAINS HIGH TO DELIVER THE SCHEME "ON TIME" IN JUNE 2022**

# EUCS – PRESENTATION OF POC EXPERIMENTATIONS

## POC ON SPECIFIC REQUIREMENTS MARCH TO SEPTEMBER 2021

# TIMELINE



# POC TEAM

- **Level Substantial**
- Evaluation of specific requirements on a C5 scope and non C5 and 3 subservices
- CAB's dependency analysis. Evaluation documentation according to proposed methodology

CenterDevice – PWC - BSI

- **Level Substantial**
- Subservices and composition with 3rd party CSP
- Transition and combination between ISO 27001, C5 and SOC2: gap analysis, organizing and delivering

Continuum GRC Inc. – Lazarus Alliance

- **Level Substantial**
- Gap analysis between Zeker Online and EUCS
- Comparison of the assessment methodology with an ISAE 3402/300 approach

ExactGroup - Secura – Agentschap Telecom

- **Level High**
- Gap analysis between a C5 evaluation and level high
- How to organize the audit in conjunction with ISA 3402 and ISO 27001

Fabasoft -SGS

- **Level Substantial**
- Gap analysis between ENS Nivel Medio and level Substantial
- Combination with ISO 27001 and ENS Nivel Medio audits

Grupo Trevenque – DEKRA - CCN

- **Level High**
- Focus on automated continuous monitoring on 2 different CSPs (Bosch and Fabasoft)

Medina

- **Level High**
- Pentesting requirements

Outscale – LNE - ANSSI

- **Level High**
- Gap analysis between SecNumCloud and EUCS level High
- Target specific controls (monitoring, pentesting) and the audit methodology

OVHCloud – LNE - ANSSI

- **Level Basic**
- Evaluation questionnaire
- Experimenting on selected requirements

Pan-Net Cloud – Deutsche Telekom

- Level **Substantial** or **High**
- Evaluation on 27001 scope
- Audit on specific requirements identified as bottlenecks

SecureMailBox

# NEXT STEPS AND THOUGHTS?

## GUIDANCE

# GUIDANCE VS. REQUIREMENTS

## Requirements

**A REQUIREMENT IS PART OF THE SCHEME, AND IT IS MANDATORY TO FOLLOW IT TO BE CERTIFIED**

Requirements are expressed with “shall”

Requirements usually keep a high enough level of abstraction

Because they are part of the scheme, requirements can only be updated every few years

## Guidance

**GUIDANCE IS NOT PART OF THE SCHEME, AND IT IS ONLY RECOMMENDED TO FOLLOW IT**

Guidance is expressed with “should”

Guidance is usually practical, and it can be updated regularly

Following guidance simplifies the relationship with the CAB, by using solutions that are known to meet the requirements

# KEY GUIDANCE DOCUMENTS

## ABOUT THE SCHEME

- Guidelines for compliance monitoring and continued compliance
- Guidance on risks and levels
- *Guidelines for users of services certified with EUCS*

## ABOUT THE REQUIREMENTS

- General guidance
- Crypto guidance
- Guidance for auditors
- Additional guidance
  - Specific guidance on logging, admin, and service providers (incident detection and response, pen testing)
- *Mappings to other schemes and standards*

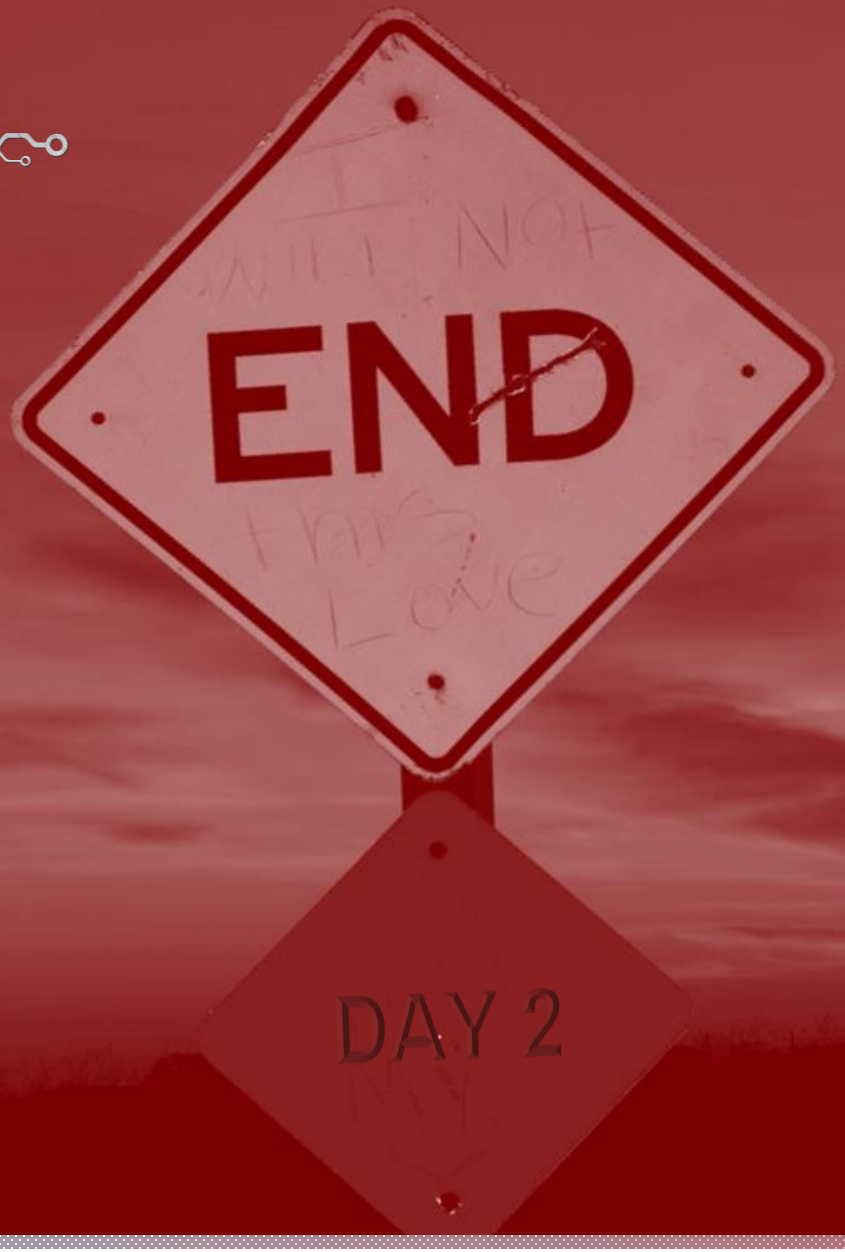
## ABOUT THE ASSESSMENT

- Checklist for EUCS Basic
- Migrating from [XXX]
  - Where XXX is C5, SecNumCloud, Zeker Online, possibly 3402 and 27001 and more
- Auditing assurance documentation
- Auditing composition
- Combining with ISO 27001 and ISO 17021
- Combining with ISAE 3402
- Composition and [XXX]

With the AHWG

With a consultant

With Member States




# QUESTIONS ?

# CONTACT


## Red Alert Labs

3 rue Parmentier| 94140 Alfortville

*contact@redalertlabs.com*

+33 9 53 55 54 11

**www.redalertlabs.com**


RED ALERT LABS
IoT Security