European CSP Security Certification

Helmut Fallmann, Fabasoft

CSP CERT WORKING GROUP CHAIRMAN


CSPCert
Warsaw 30 September
2019
Final Public-Private recommendation for a
European Cloud Security Certification Scheme

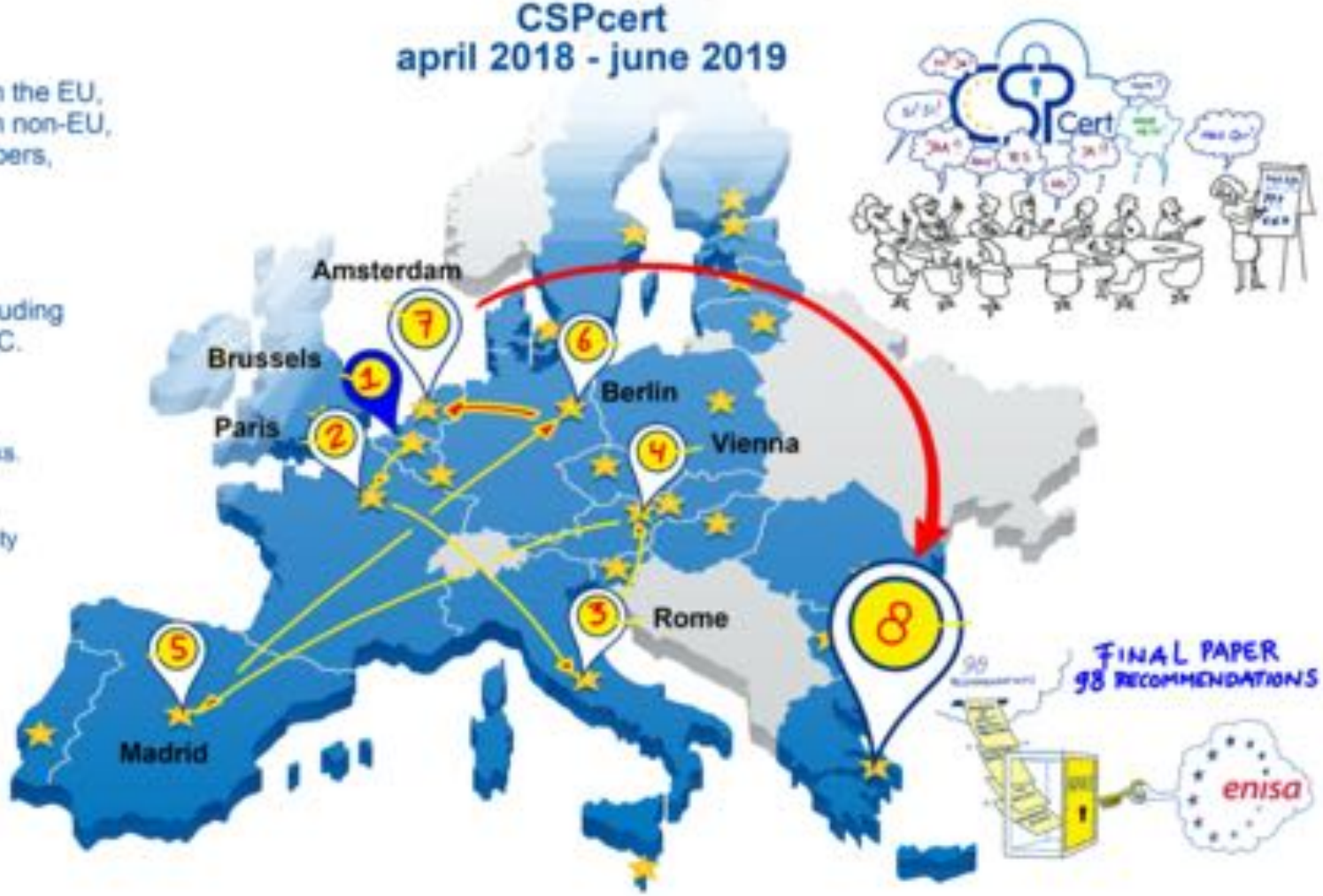
CSPcert
april 2018 - june 2019

52 members from the EU,
16 members from non-EU,
32 Drafting members,
10 authors,
7 contributors,
2 co-chairs,
1 reporter,
34 observers including
ENISA and the EC.

Milestone 1.
Criteria based on
study of 6 frameworks.

Milestone 2.
3 proposed conformity
assessments
- evidence based
- iso based
- isae based

Milestone 3
12th of June 2019
in Amsterdam,
presentation of
the final advise.



Cloud Computing Assurance Levels (CCAL)

Prof. William Ochs
Certification Enablement Manager
Cisco Global Certifications
USA

CCAL Overview

- Scope of the Certification
- Refined Objectives for the European CSP Service Certification
- Assurance Levels
  - Role of Risk Management in Determination
  - Characteristics and Requirements for the Assurance Levels
- Ensuring EU-wide Recognition of Certificates through Consistency of Assurance Levels

CCAL Overview

- CSPCERT WG Defines 26 Recommendations for ENISA and the EU Commission Related to Certification Assurance Levels
- Recommendations are tied directly to the European Union Cybersecurity Act (EUCA)
- CCAL Focus Primarily on Article 51 and Article 52 of the EUCA
- Provides for Examples that could be utilized in the selection of a Certification Level of Assurance based on risk scenarios and risk assessments taken by an end-user for a Cloud Service
- Provides for CSP certification perimeters and the addition of new sectoral requirements or overlays to the certification
- Provides for Cybersecurity act's assurance requirements and their correspondence to the different assurance levels

CCAL: Scope of the Certification

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

CSPCERT, Milestone 3.

CCAL: Refined Objectives for the European CSP Service Certification

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

CSPCERT, Milestone 3.

CCAL: Refined Objectives for the European CSP Service Certification

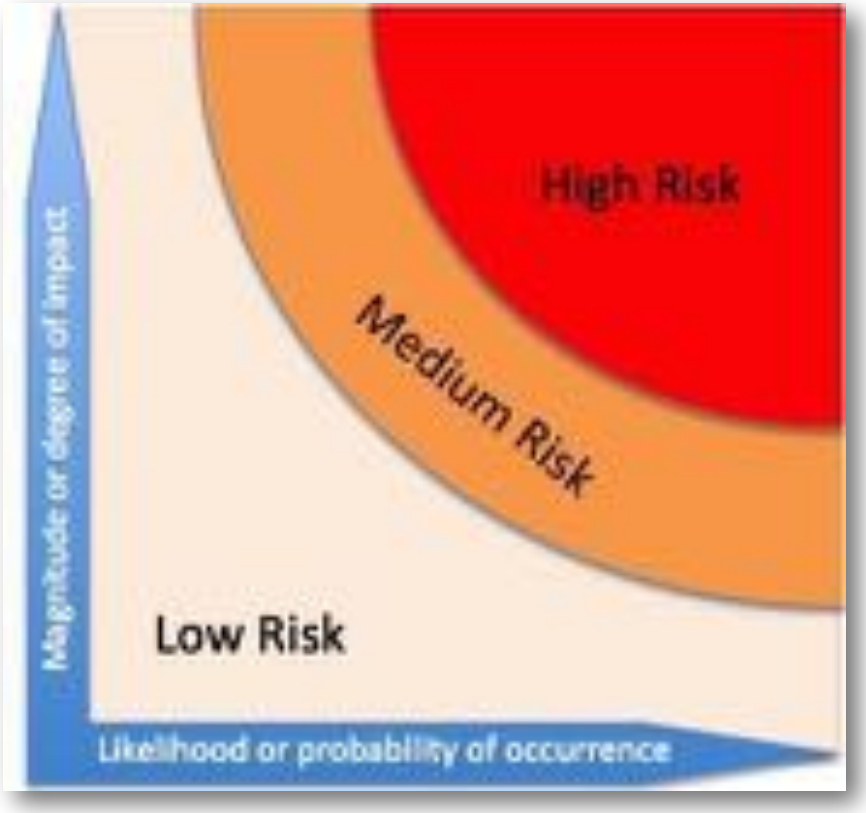
- Focused on Article 51 of EUCA
- First 10 Recommendations Fall Under Article 51
- All CSPCERT Recommendations are numbered and come with a Justification statement.

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

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

CCAL: Assurance Levels and Risk Assessment Correlation

- Focused on Article 52 of EUCA
- Recommendations 11-21, Fall Under Article 52
- "*Performing a proper risk analysis requires that both dimensions need to be considered and assessed. Based on the outcome of the risk assessment, a required level of assurance can be determined.*" CSPCERT, Milestone 3.



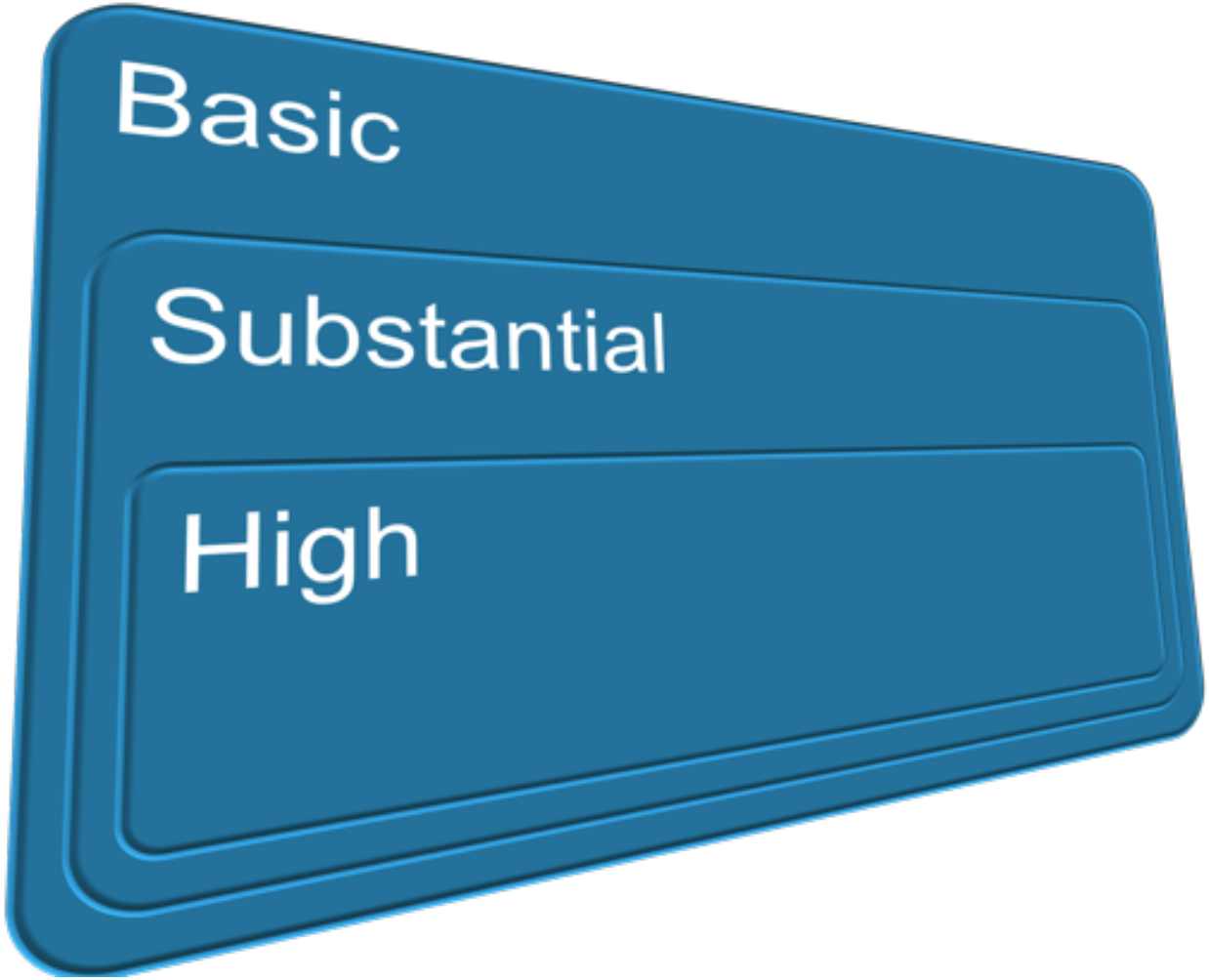
CCAL: Assurance Levels

Defined Areas Impacted by Recognized Risks

CCAL: Assurance Levels

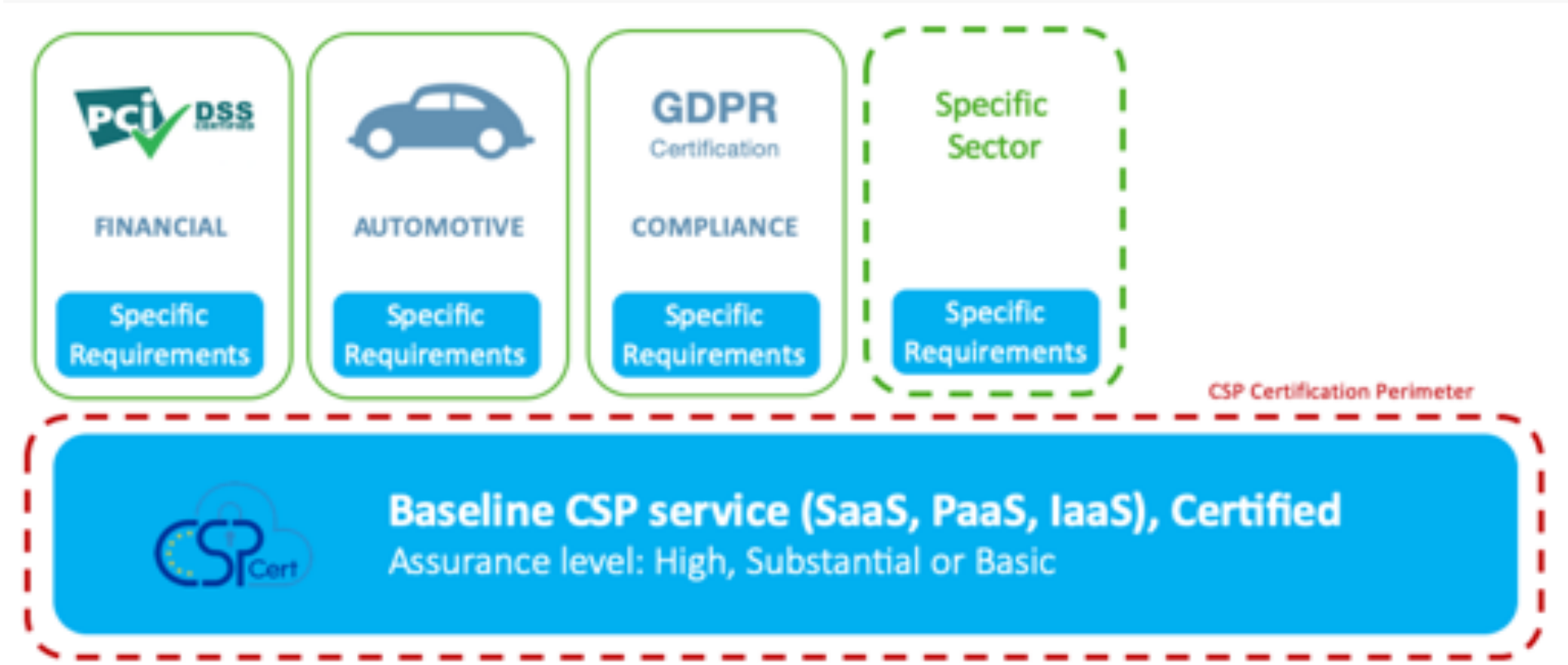
Defined Areas Impacted by Recognized Risk

CCAL: Assurance Levels as Defined in EUCA Article 52



CCAL: Assurance Levels

CSP Certification Perimeter & Addition of New Sectoral Requirements



CCAL: Ensuring EU-Wide Recognition

- Recommendations 22-26 Focus on Level of Trust, Fidelity, and Certificate Acceptance
- Introduce the Concepts of Audit Level of Detail relevant to Assurance Level
- Introduce Peer Review Mechanisms
- Introduce Governance's Import (Addressed in Detail in SGOV)
- Recommends NCCA Endorses the Final Audit Reports and Issuance of Certificate

Cyber Security Act Requirements (CSAR)

Tom Vreeburg
Independent IT Risk and Assurance professional
Advisor to the board of NOREA.
NOREA
Netherlands

CSAR Part

EU Cybersecurity Act (EUCA) provides cybersecurity certification framework (Section III, Art 46 a.o.)

CSPCert provides recommendations for ENISA to prepare a European Cybersecurity Certification Scheme for Cloud Service Providers

EUCA, Art 46: ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

Requirements for a scheme in particular in EUCA art 54 and 55

EUCA Art 54

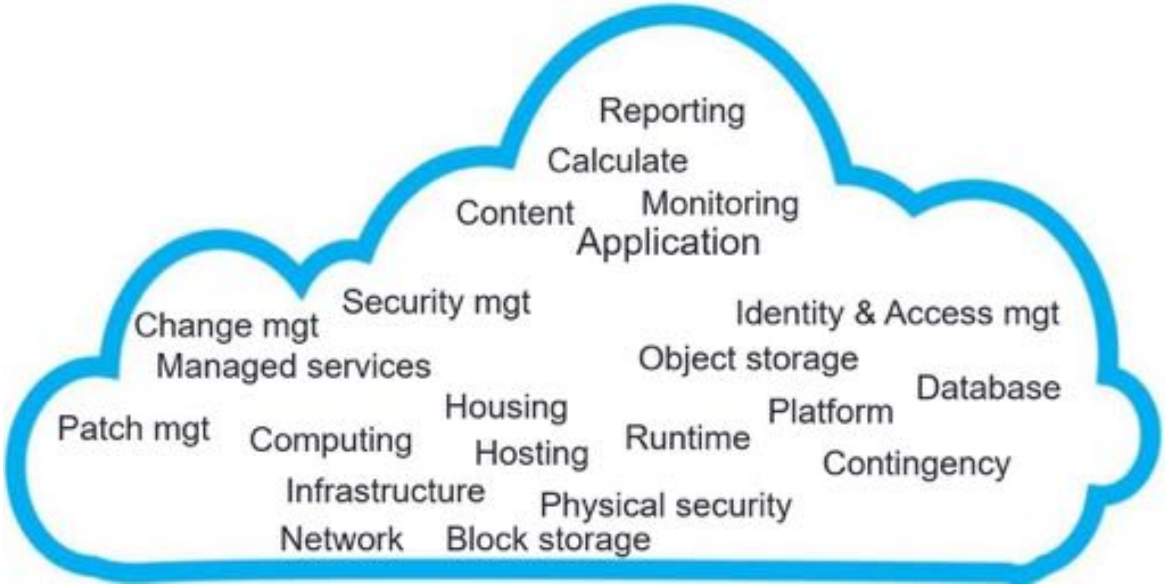
Elements of European cybersecurity certification schemes

22 elements provide minimum requirements

CSPCert added 20+ recommendations to provide guidance to ENISA how to detail these elements in the EU Cybersecurity Certification Scheme for Cloud Service Providers

Scope

- Purpose of the scheme:
  - Provide stakeholders with statement on scope, reliability and security of cloud service
  - Enhance credibility/confidence/ trust of statement by CSP
- Scoping in a cloud environment



Information provided by Cloud Service Provider

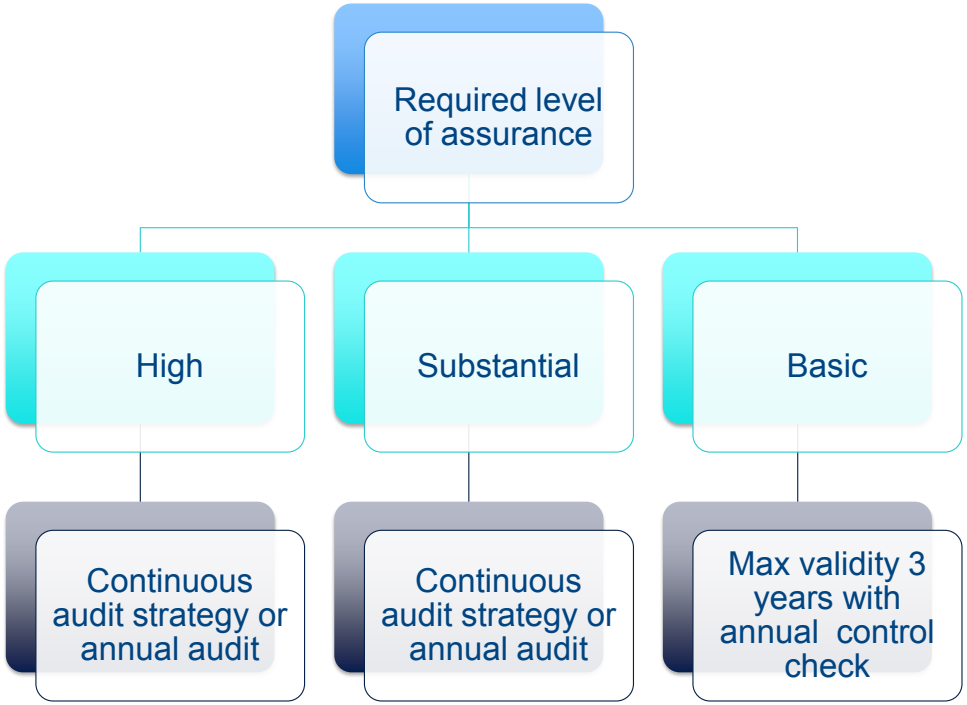
Information needed for issuance of the certificate

Identification
CSP's Conformity statement
CSP's description of the service
•Control objectives, related controls and tests of controls
Other information

Supplementary cybersecurity information (EUCA Art 55)

Consequences of non-compliance with requirements of the scheme

Maximum period of validity



Scheme Governance (SGOV)

Thomas Niessen

Managing Director
Kompetenznetzwerk Trusted Cloud e.V.
Germany

SGOV Part

- Commons parts between all assurance levels
  - Committee and groups
  - Complaints management
  - Peer Review
  - Community management

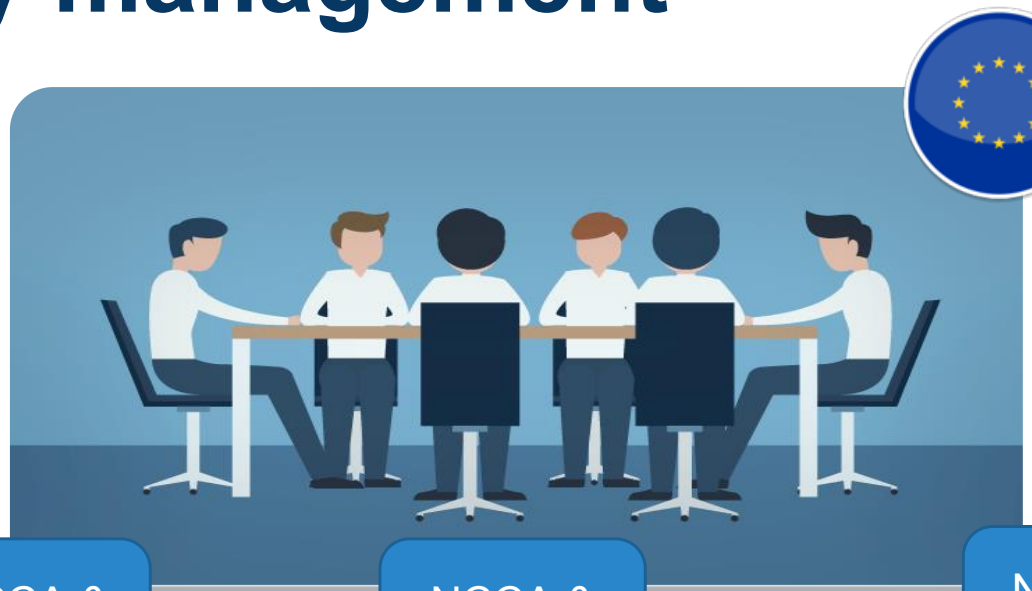
- Specific governance recommendations
  - For each assurance level
  - Basic, Substantial and High

Committee and groups (EU level)

Complaints Management

Peer reviews

Community management

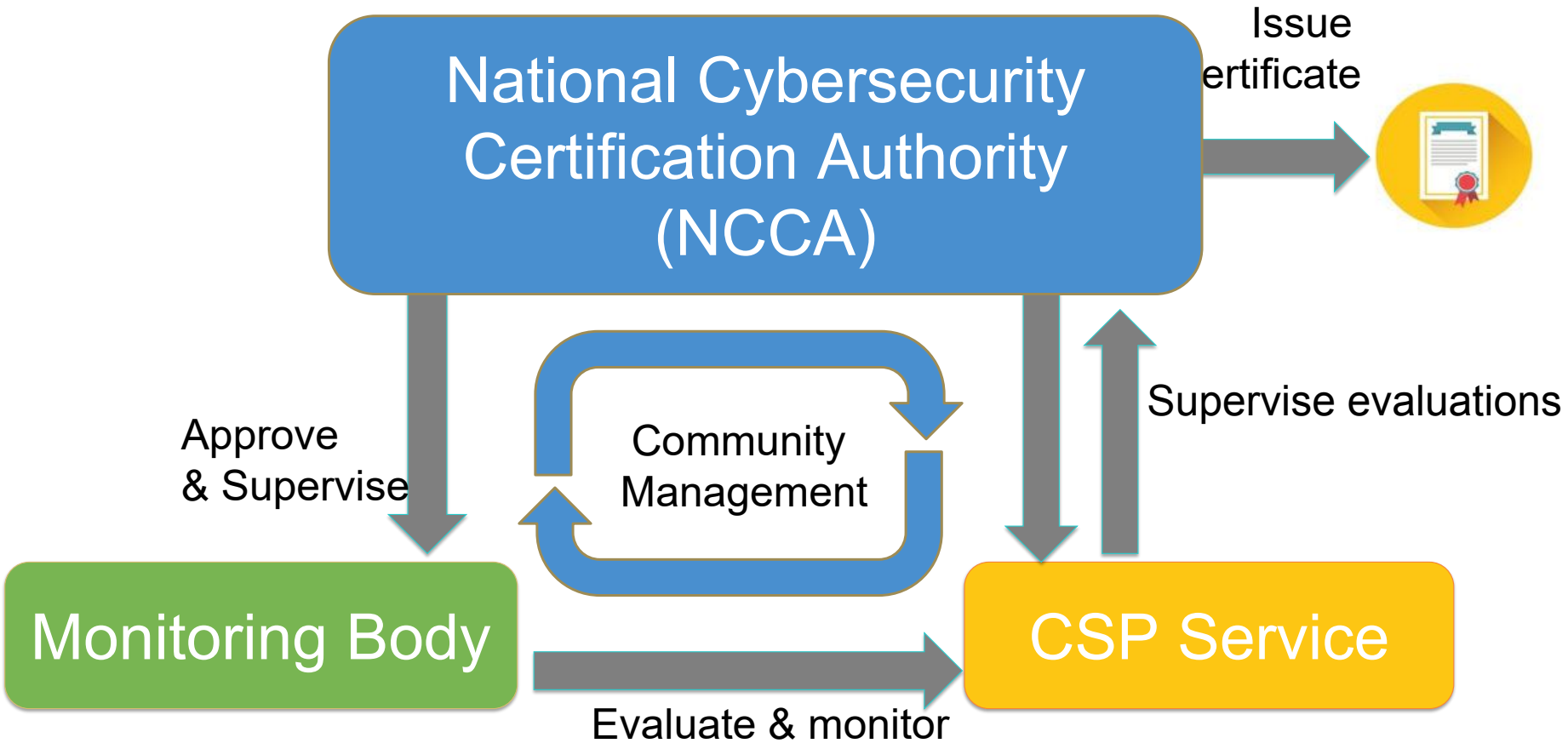


NCCA & Experts

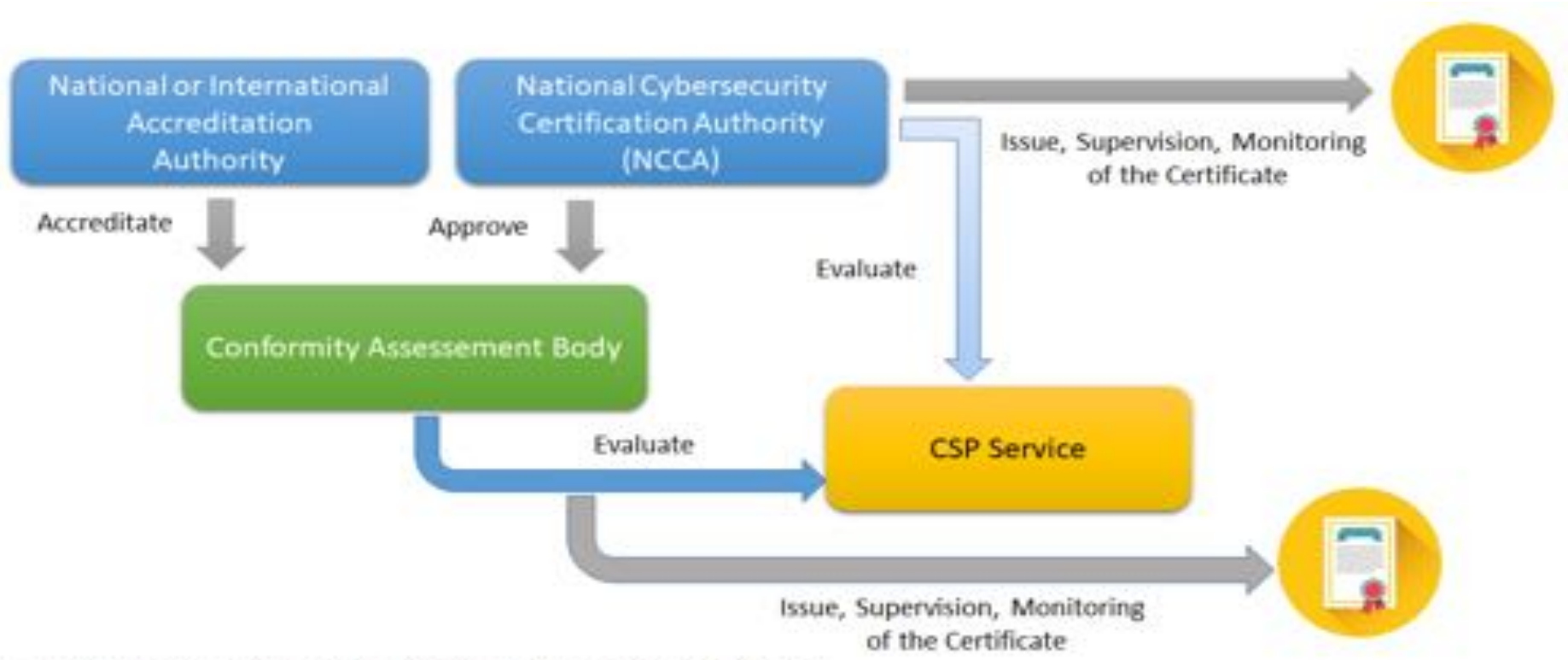
NCCA & Experts

NCCA & Experts

Assurance level Basic

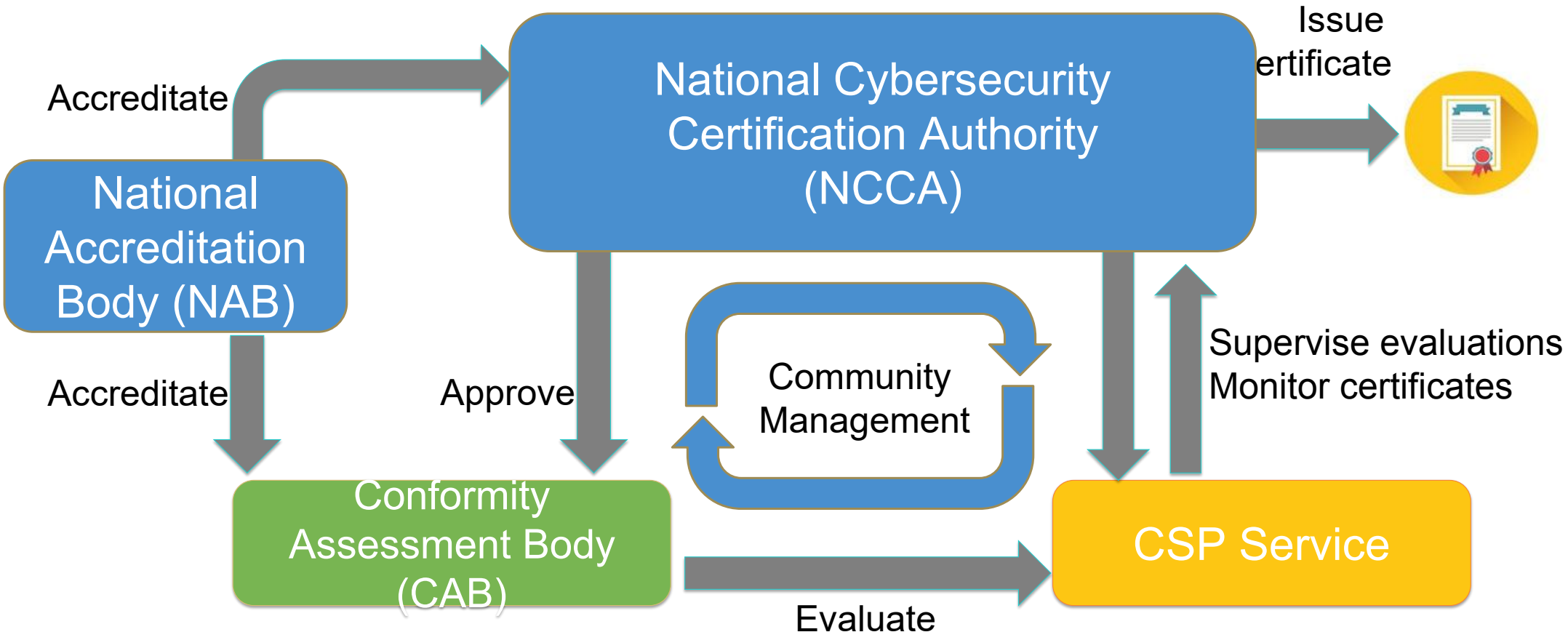


Assurance level Substantial



1 – The NCCA can have an evaluation step as part of final certification in some instances for Substantial.
2 – The NCCA can delegate or approve a Conformity Assessment Body to perform CSP Evaluations.
3 – Where the NCCA has absorbed responsibility for evaluation, they inherit responsibility for supervision and monitoring of the issued certificate.

Assurance level High



Conclusion and recommendations

Bert Tuinsma
Chairman of Zeker-OnLine
Issuer of trust certificates to Cloud Services Providers
The Netherlands

General recommendation

To include the **development of an EU-wide cloud security certification scheme** in the EU rolling work programme for European cybersecurity certification framework under the EUCA


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

To request ENISA to prepare a candidate scheme on the **basis of the present proposal**

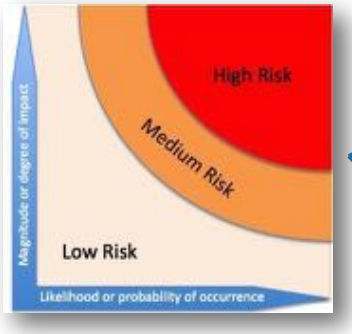
General recommendation

CSPCERT does not recommend a completely new certification scheme but rather for a scheme based on existing practices/schemes/standards used by the industry and internationally recognized

Cloud Computing Assurance Levels (CCAL)

Assurance levels required

3 **levels of assurance**: Basic, Substantial and High, depending on the risk level associated



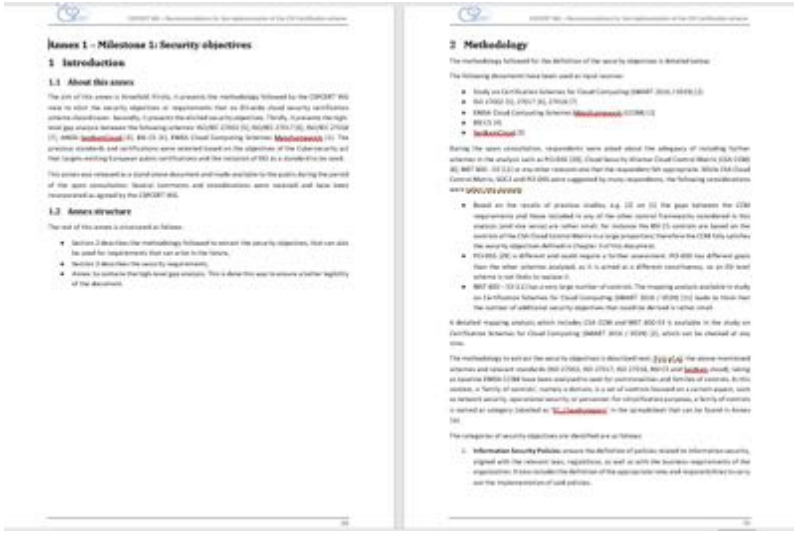
Clear guidance on how to perform this **risk assessment** and **link the assurance level** to the cloud service

A **description** of what the basic/substantial/high assurance level indicates

Examples of which level of assurance should be associated with which service

Cloud Computing Assurance Levels (CCAL)

Evaluation criteria



Annex 1 – Milestone 1: Security objectives

1 Introduction

1.1 About this annex

1.2 Annex structure

2 Methodology

Keep a **similar taxonomy** and update it when appropriate

Keep a **similar methodology** for the inclusion of new controls and update it accordingly

Defined a set of Security Objectives, with a taxonomy and a methodology to include new ones, when required

Cloud Computing Assurance Levels (CCAL)

Conformity Assessment Methodologies

3 conformity assessment methodologies (CAM)

- Evidence-based
- Third-party
  - ISO-based
  - ISAE-based

Evaluate the possibility of including **continuous monitoring** for High

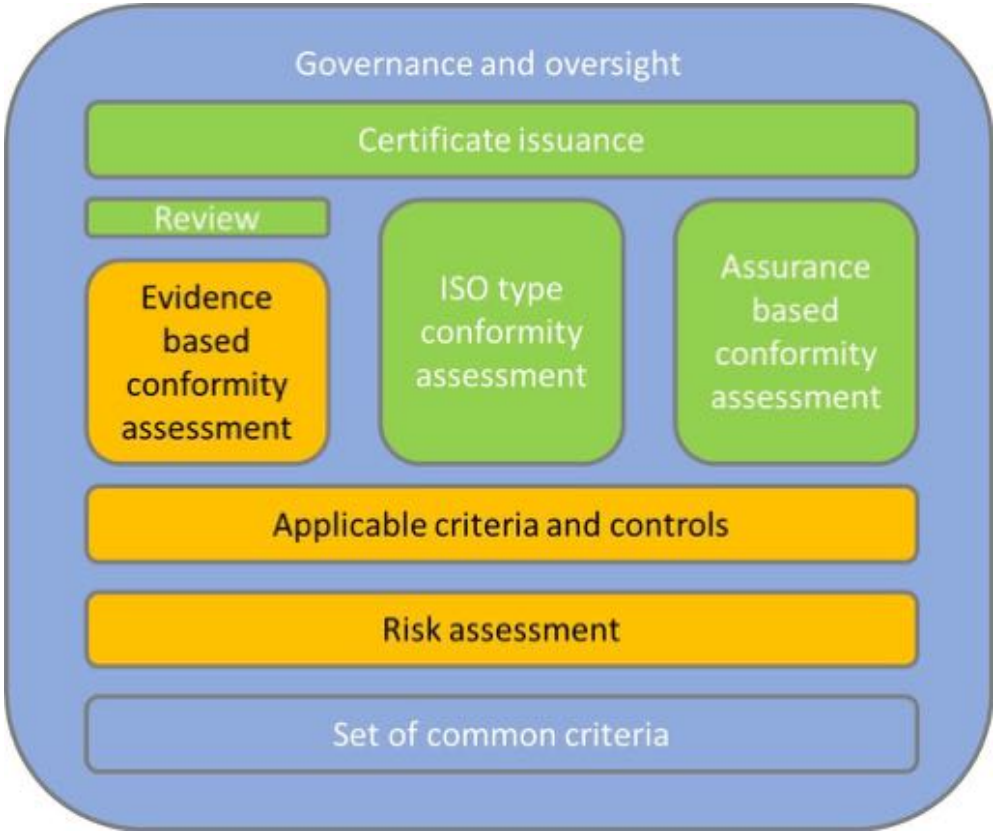
Frequency of renewal and what triggers it

To reduce the level of bias, **assess third-party conformity assessment methodologies for safeguards** to ensure a common level of trust

Clear **guidance on the** required **procedures** and **criteria** per assurance level

CAMs must measure **operational effectiveness in S and H,** and not merely control existence

Summary


Governance and oversight
Certificate issuance
Review
Evidence based conformity assessment
ISO type conformity assessment
Assurance based conformity assessment
Applicable criteria and controls
Risk assessment
Set of common criteria

cspcerteurope@gmail.com

www.cspcert.eu