Workshop:
How to build and operate a certification body and testing laboratory in the context of the EUCC

2.-3.11.2022

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

WORKSHOP EUCC

Národní úřad pro kybernetickou a informační bezpečnost

PROGRAM:

8:00 – 8:30	Registration
8:30 – 8:35	Organizational instructions
8:35 – 8:45	Welcome speech
8:45 – 9:15	Proposal for Cyber resilience act
9:15 – 10:00	Why and how to become a CAB for the EUCC scheme
10:00 – 10:15	Coffee break
10:15 – 11:45	How a Certification Body operates Part 1: in the context of EUCC Part 2: in the context of ISMS and EUCS
11:45 – 12:45	Lunch break
12:45 – 14:15	How to build and operate a test. lab. in the context of EUCC
14:15 – 14:30	Coffee break
14:30 – 16:00	How to build and operate a test. lab. in the context of EUCC
16:00 – 16:15	Closing remarks

ORGANIZATIONAL INSTRUCTIONS

- Please, turn off your cell phones
- Emergency exit
- Cofee break
- Lunch break:
  - location is on the back side of your program
  - paid for by the organizers
  - please, remember your choice
- All the available materials will be sent to all persons on our mailing list

WELCOME SPEECH

M. SMRČKA / A. KUČÍNSKÝ

Cyber Resilience Act proposal

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

2 November 2022

Adam Botek
Cyber attaché

❖ Two goals of Cyber Resilience Act

1) Reducing number of vulnerabilities in products with digital elements
2) Equipping users with better information

❖ Based on New Legislative Framework

❖ Horizontal nature

➢ Interacts with IA Act, machinery products Regulation, Cybersecurity Act, etc.

Scope

Products with digital elements

- All hardware and software connectable to other devices or network

- HW: Laptops, smartphones, routers, sensors, SCADA
- SW: operation systems, mobile apps, video games
- Components: CPU, software libraries

Critical products

- For functionality features or intended use
- Secure crypto processors, firewalls and routers for industrial use

Essential requirements

- **Requirements related to properties of products**
  - Delivery without any known vulnerabilities

  + on the basis of risk assessment:
  - Protection of data and availability of essential functions
  - Ensuring that vulnerabilities can be addressed through security updates
  - …

- **Requirements related to vulnerability handling** (for at least 5 years, or expected lifetime of a product, whichever is shorter)
  - Identification and documentation of vulnerabilities
  - Regular testing of products
  - Vulnerability handling
  - Disclosure of patched vulnerabilities

Economic operators and their obligations

- **Economic operators** = manufacturers, importers, distributors

- **Obligations**
  - Fulfilling essential requirements
  - Informing users
  - Drawing up a technical documentation
  - Affixing CE marking
  - Reporting known vulnerabilities and incidents to ENISA

Conformity assessment

- **‚Non-critical" products** (90 % products)
  - Self-assessment (module A)

- **Critical products**
  - Class I: self-assessment possible only while applying harmonized standards, common specifications or certification schemes under Cybersecurity Act/ third-party assessment
    Class II: third-party assessment

- **Empowerment of the Commission**
  - Specification of CSA certification schemes to be used for presumption of conformity
  - Adoption of common specifications, if harmonized norms are absent or insufficient

Market surveillance

- **Procedures concerning products presenting a significant cybersecurity risk**
  - At national level
  - At Union level

- **Measures**
  - Requiring adoption of corrective actions
  - Ordering withdrawal or recalling of a product from the market

  - In case of non-compliance, possibility of imposing sanctions

Adam Botek

Cyber attaché

E-mail: a.botek@nukib.cz

DISCUSSION

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU CYBERSECURITY CERTIFICATION

WHY AND HOW TO BECOME A CAB

Philippe Blot
Head of Cybersecurity Certification sector
Market, Certification & Standardisation Unit
ENISA, The European Agency for Cybersecurity

02 | 11 | 2022

EU CERTIFICATION: ALL YOU NEED TO KNOW

EU Certification: All you need to know
https://www.youtube.com/watch?v=03zxrb2Fc0A

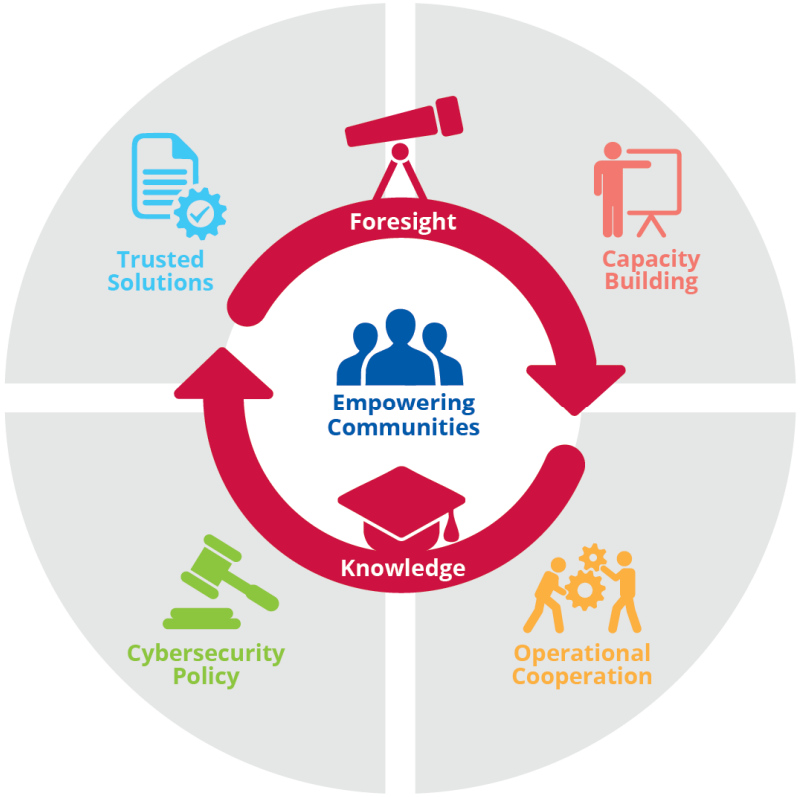
You missed the first episode?
What's in for Conformity Assessment Bodies (CABs)**?**
https://www.youtube.com/watch?v=vabWKHGrjGM

WHO WE ARE

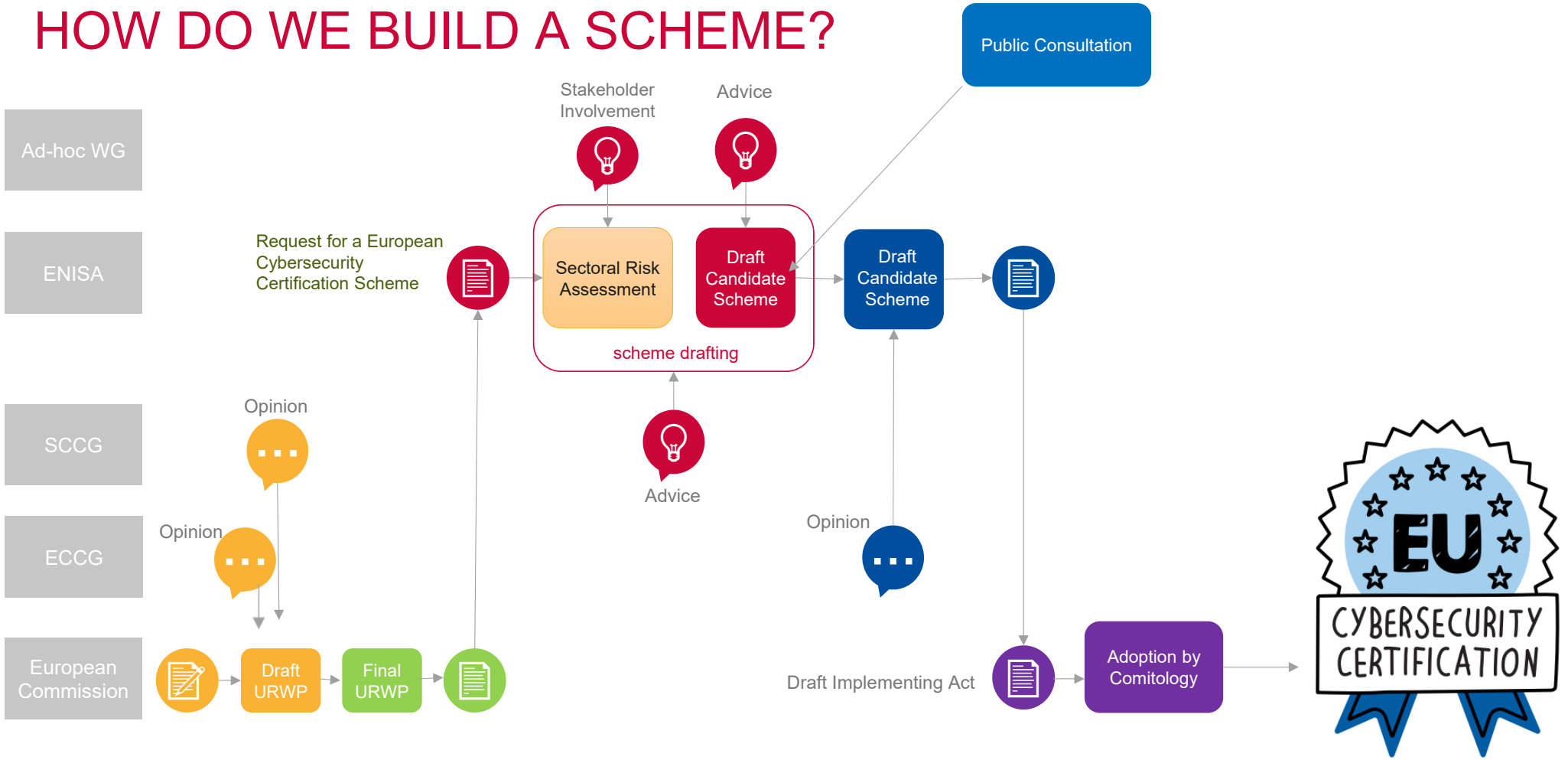
The European Union Agency For Cybersecurity is dedicated to achieving a high common level of cybersecurity across Europe.

- ENISA plays a key role in enabling the Union's ambition to **reinforce digital trust and security across Europe**, **together** with the Member States and EU bodies.

- By bringing communities together, the Agency continues to successfully contribute **to strengthening Europe's preparedness and response capabilities** to cyber incidents.



HOW DO WE BUILD A SCHEME?



EUCC: AN HORIZONTAL ICT PRODUCTS SCHEME

Based on international standards

Common Criteria & CEM

ISO/IEC 17065 & 17025 for the accreditation

Horizontal

Defines the “how to certify”

The “what to certify” is for risk owners to define through Protections Profiles or individual security targets

2 assurance levels

As defined in the European Cybersecurity Act

‘substantial’ (AVA_VAN.1 & 2)

‘high’ (AVA_VAN.3, 4 & 5)

All levels based on an assessment by an accredited third-party

EUCC : CURRENT WORK IN PROGRESS

- **Implementing Act (ENISA support to the EC**) based on the candidate scheme, including relevant annexes
- **Maintenance strategy**
- **Catalogue of national supporting documents** that may become new mandatory requirements
- **ENISA website dedicated to certification,** promoting schemes and certificates
- **Harmonised cryptographic** evaluation procedures

EUCS SCHEME : GENERIC APPROACH TO THE CLOUD

All capabilities

Based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Preferred for clarity to references to IaaS, PaaS, SaaS, XXaaS

No mention of deployment model

Horizontal

Defines a baseline of requirements that are applicable to all services.

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

3 assurance levels

As defined in the European Cybersecurity Act

'basic' → CS-Basic

'substantial' → CS-Substantial

'high' → CS-High

All levels based on an assessment by an accredited third-party

EU5G SCHEME

Phase 1

Ongoing

Until Q3

- **3 Workstreams**: as-is transposition of GSMA NESAS, SAS-SM, SAS-UP and eUICC, plus risk assessment and gap analysis.
- Then **feedback to the ECCG**

Phase 2

To Follow

- **Development of the candidate scheme**
- **Permanent coordination with the NIS CG** to reuse their elements for the benefit of the EU5G scheme

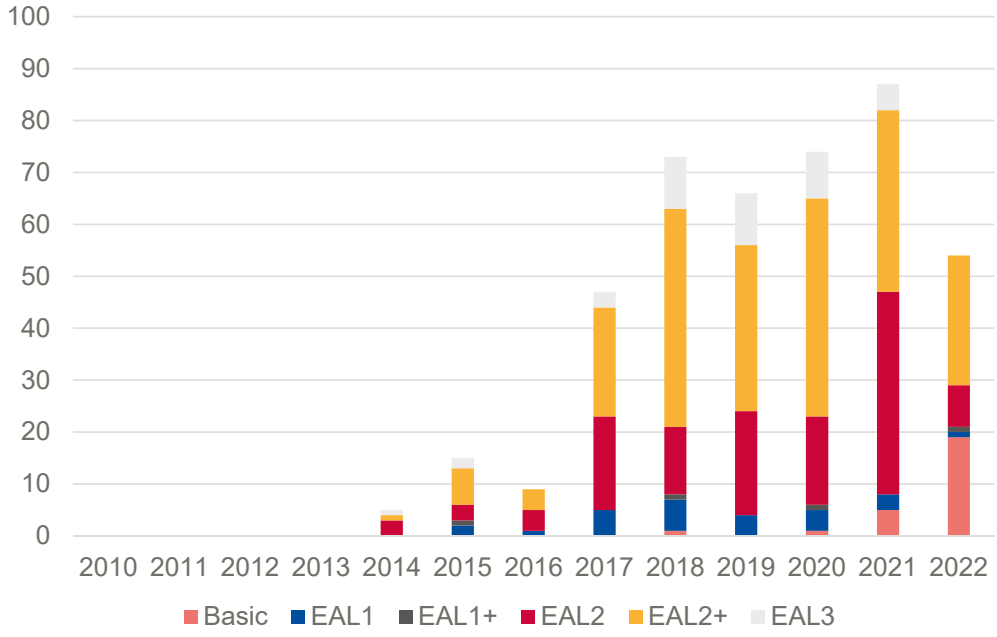
Challenges:

- Estimate the equivalent CSA assurance level of existing GSMA schemes and ensure consistency
- Conduct risk assessments to potentially ensure technical comparability between GSMA/3GPP and EU schemes
- Future maintenance of the scheme

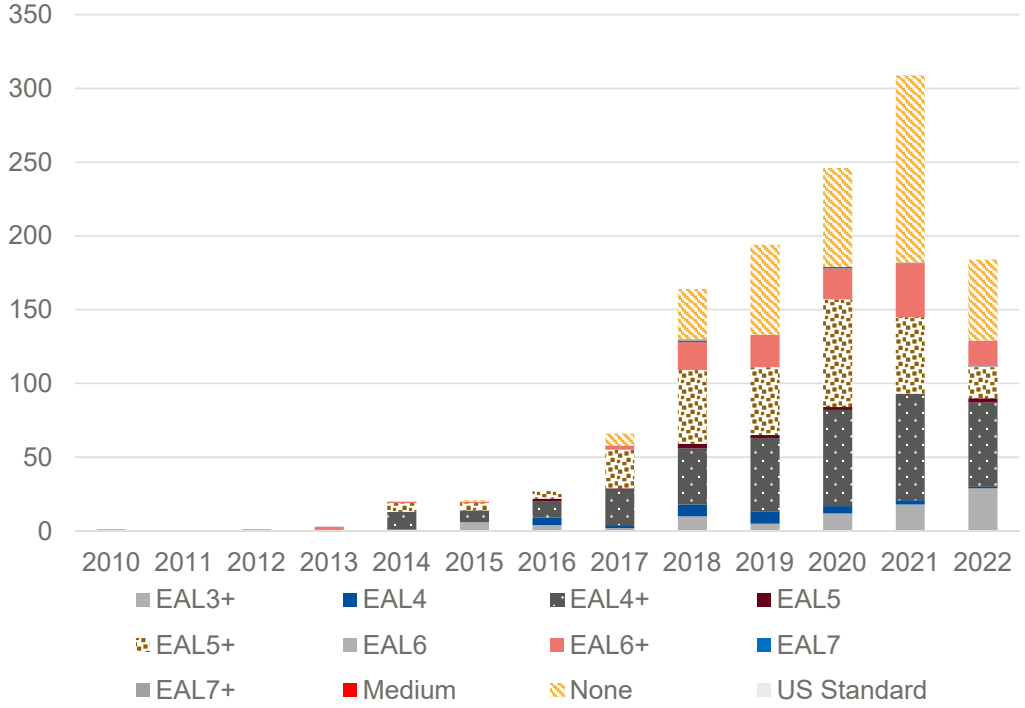
CURRENT CCRA AND SOG-IS MARKETS

Total = 1662

Certified Products by assurance level and date (from CC Basic to EAL 3)



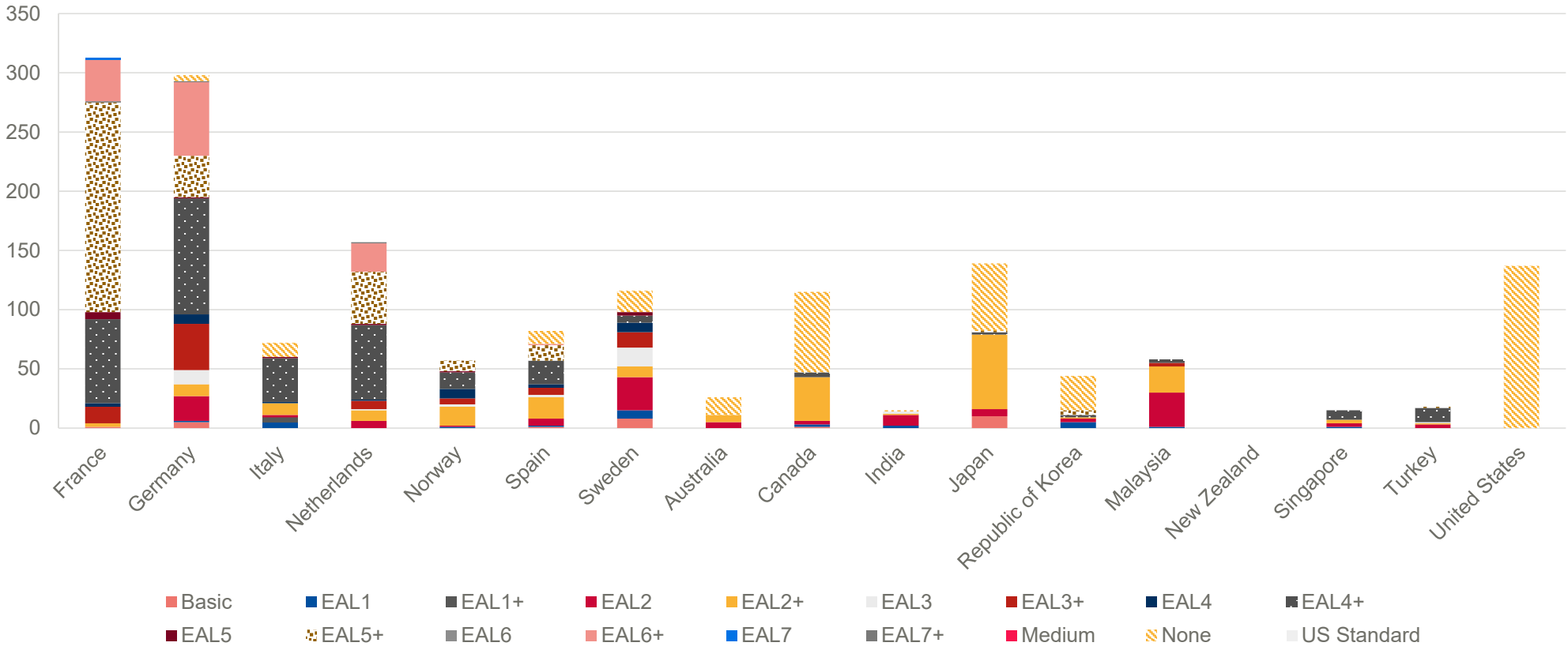
Certified Products by assurance level and date (from EAL 3+)



Based on Certified Products List – Statistics : New CC Portal (commoncriteriaportal.org)

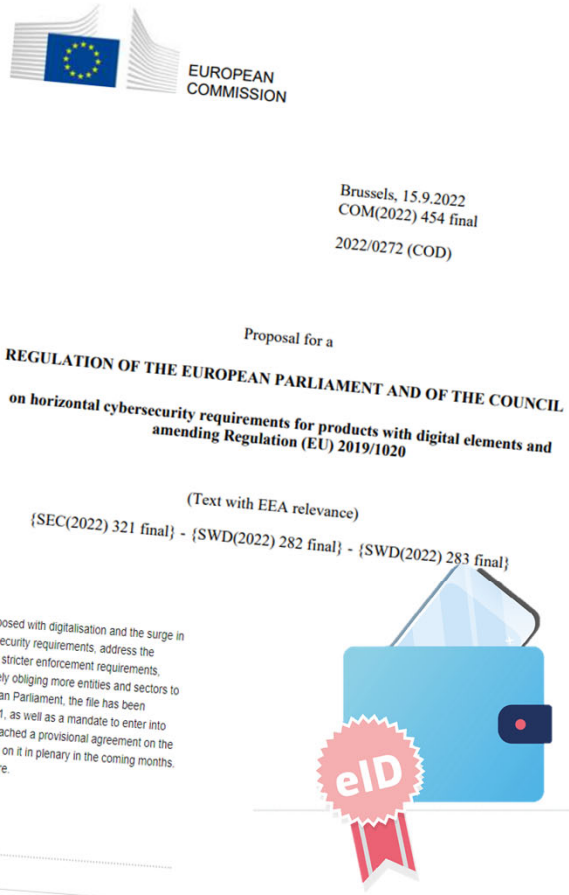
CURRENT CCRA AND SOG-IS MARKETS

Total = 1662



Based on Certified Products List – Statistics : New CC Portal (commoncriteriaportal.org)

REGULATIONS TO COME



EUCC REQUIREMENTS REGARDING THE VENDORS

Not so many requirements on the what to certify (the scheme is more on the how to certify), still some (1/2):

On the Security Target:

- mandatory inclusion of SARs AVA_VAN (with all related dependencies), ATE_IND & ALC_FLR
- consider the level of risk associated with the intended use of the product and include the security functions contained in the product that support the security objectives defined in Article 51 of the Regulation (EU) No 2019/881 relevant to that ICT product

Existing SOG-IS technical domains and related requirements (MSSR, …) are kept (specific PPs foreseen to address specific cases

Applicants for certification shall provide the CB and ITSEF with:

- the link to their website containing the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) No 2019/881 with a view to having all necessary information included in the EUCC certificate;
- a description of the vulnerability handling and vulnerability disclosure procedures, and
- if within the scope of certification, a description of the patch management mechanism

EUCC REQUIREMENTS REGARDING THE VENDORS

Not so many requirements on the what to certify (the scheme is more on the how to certify), still some (2/2):

The applicant for certification shall undertake commitments:

- to provide the certification body and the ITSEF with reliable information;
- not to promote an ICT product as certified under the EUCC before the EUCC certificate has been issued;
- to promote an ICT product as certified only with respect to the scope set out in the EUCC certificate;
- to cease immediately the advertisement of the certification of the ICT product or Protection Profile in the event of a suspension, withdrawal or expiry of the EUCC certificate;
- to ensure that the ICT products sold in connection with the EUCC certificate are strictly identical to the ICT product subject to the certification;
- to respect the rules of use of the mark and label established for the EUCC certificate

EUCC CERTIFICATES

- **Maximum period of validity:** five years for products certificates, no limit for PPs
- **NCCAs will monitor certificates** based on sampling, and on non-conformity/compliance of certified products and CBs/ITSEFs
- **CBs and ITSEFs will also have monitoring activities**
- **Vendors will have to monitor vulnerability information,** and to handle non compliances and vulnerabilities
- **A label is foreseen** to promote the certificates
- **Mutual recognition** with third countries is foreseen

EUCC REQUIREMENTS REGARDING THE CABS

Notification of CABs based on:

- **Substantial level:** accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025
- **High level:** accreditation of CBs according to ISO/IEC 17065 and of related ITSEFs according to ISO/IEC 17025, plus their authorisation by a NCCA

CB and ITSEF: appropriate competence management system for the personnel based on ISO/IEC 19896-1.

Specific for ITSEFs:

- ISO/IEC 17025 complemented by ISO/IEC 23532-1 (lab) and ISO/IEC 19896-3 (evaluators)

Foreseen promotion of notified CABs: ENISA Certification website + mark & label

EUCC REQUIREMENTS REGARDING THE CABS

Difference between accreditation and authorization: review* by the NCCA of the CB (resp. ITSEF):

- Competences and expertise to certify (resp. evaluate)
- Capability to protect confidential and sensitive information

*Based on structured interviews and a review of two pilot certifications (resp. evaluations) performed by the certification body (resp. ITSEF)

Specific for ITSEFs:

- Requirements defined for Technical Domains evaluations defined in SOG-IS documentation
- For AVA_VAN.3 evaluations: ENISA guidance available

Authorisation duration: 3 years

Peer assessment of CBs (including associated ITSEFs)

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711

certification@enisa.europa.eu

www.enisa.europa.eu

DISCUSSION

15 min

Federal Office
for Information Security

How to operate as a Certification Body in context of EUCC

Klementina Geyer
2-3rd November 2022

Agenda

1. Brief profile of the BSI
2. The Common Criteria Certification Infrastructure in Germany
3. Establishment of the EUCC Ecosystem
4. Supporting Activities for Level “substantial”
5. Outlook and Next Steps

1. Brief profile of the BSI

Established
1 January 1991

197 million euros budget 2021

Posts in 2021

1550 ↗

116 new jobs compared to previous year

BSI presence

- Sites
- Offices
- Liaison offices

Brussels

Furthermore, the BSI has long been playing a key role at the international levels, including in close cooperation with bilateral partners and in multilateral fields of action relating to the EU and NATO.

Federal Office
for Information Security

Organisation

As of: 15 December 2021

Executive Staff — **President**, **Vice President**

Division Z Central Tasks	Division TK Technical Centres of Excellence	Division KM Information Assurance Technology and IT Management	Division OC Operational Cyber Security	Division SZ Standardization, Certification and Cyber Security of Telecommunication Networks	Division DI Cyber Security for Digitization and Electronic Identities	Division BL Consulting for Federal, State and Local Governments	Division WG Cyber Security for the Private Sector and Society
Branch Z 1 Central Tasks 1	**Branch TK 1** IT Systems	**Branch KM 1** Classified Information System Approvals	**Branch OC 1** Detection	**Branch SZ 1** Standardization, Certification Policy, Supervision	**Branch DI 1** Cyber Security for Electronic Identities (eID)	**Branch BL 1** IT Security Consulting and Security of Classified Material	**Branch WG 1** Cyber Security for Critical Infrastructures
Branch Z 2 Central Tasks 2	**Branch TK 2** IT Infrastructures	**Branch KM 2** Classified Information System Requirements	**Branch OC 2** CERT-Bund	**Branch SZ 2** Certification Processes	**Branch DI 2** Cyber Security for Digitization	**Branch BL 2** Client Management and Law	**Branch WG 2** Cyber Security for the Private Sector
		Branch KM 3 IT Management	**Branch OC 3** IT-Security Situational Awareness	**Branch SZ 3** Cyber Security in Mobile Infrastructures and Chip Technology		**Branch BL 3** Information Security of Consolidated Federal Computing Centres and Networks	**Branch WG 3** Digital Consumer Protection, Cyber Security for Society and Citizens

Division SZ– Standardization, Certification and Cybersecurity of Telecommunication Networks

SZ 1 – Standardization, Certification Policy, Supervision	SZ 2 – Certification Processes	SZ 3 – Cyber Security in mobile Infrastructures and Chip Technology
SZ 11 Standardization Strategy and Investment Reviews (AWG)	SZ 21 Hardware Certification	SZ 31 Infrastructure Security for Telecommunication Networks, 5G
SZ 12 Recognition and Certification of Bodies and Persons	SZ 22 Software Certification	SZ 32 Requirements for and Auditing of Telecommunication Networks, 5G
SZ 13 BSI Standards and IT-Grundschutz	SZ 25 Certification According to Technical Guidelines	SZ 33 Certification of Network Components and Accelerated Security Certification
SZ 14 Expert Committee Work and QM for Evaluation and Certification Processes		SZ 34 Chip Technologies and eID Technologies for mobile Platforms
SZ 15 Market Surveillance of certified Service Providers and Products		SZ 35 Granting of IT Security Labels

The Common Criteria Certification Body by Numbers

Operation as **2** Certification Sections

approx. **20** Certifiers

8 Licenced ITSEFs as part of the Scheme

~90 Certification Procedures per Year

5 Administration Officers

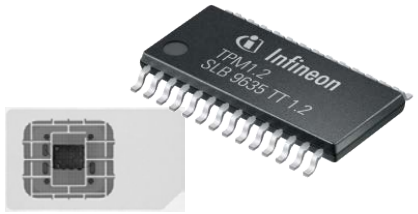
Active Work in more than **15** Working Groups

Certified Products at the BSI

Operating Systems, Application Servers, DBMSs

Health Professional Card

Digital Tachograph (EU)



Secure Elements

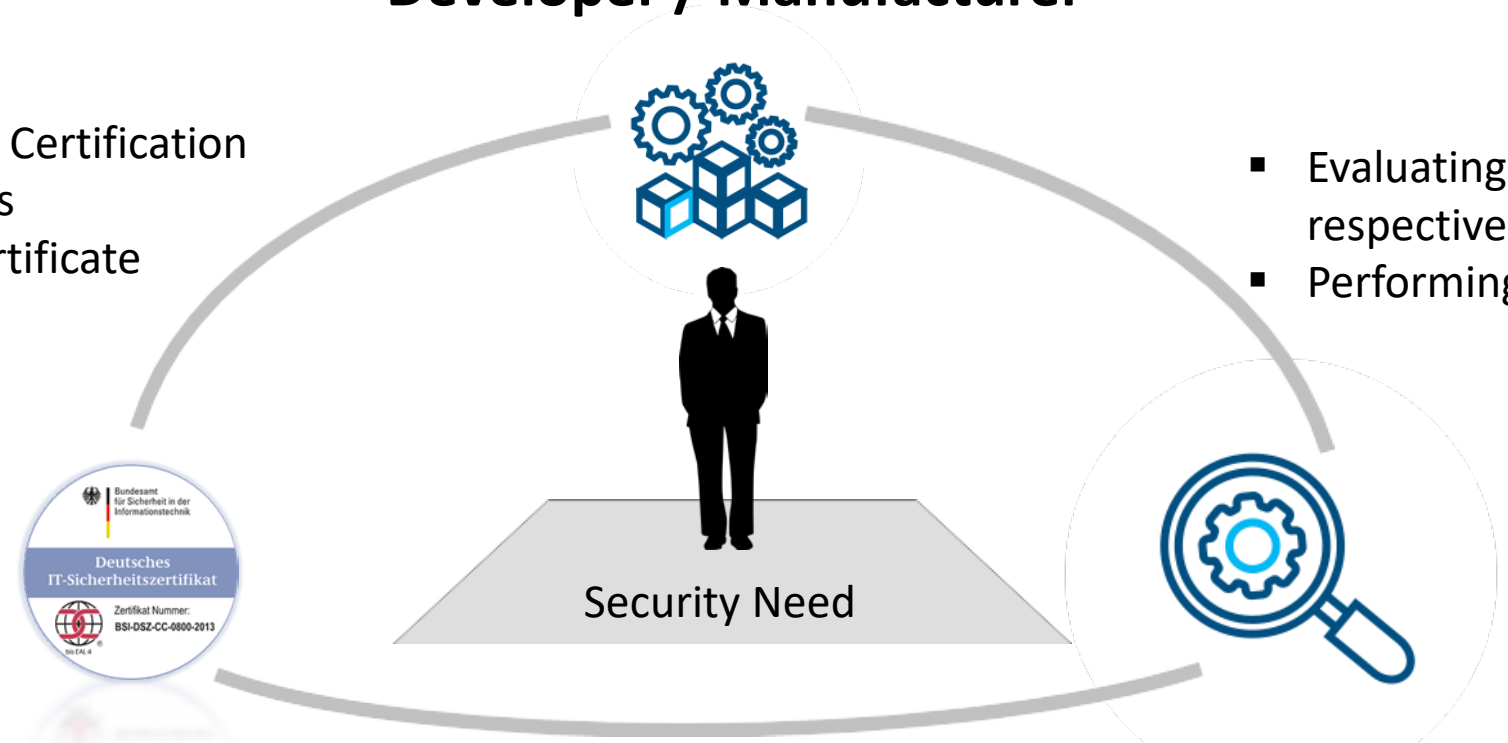
Electronic IDs and Readers

Federal Office for Information Security

The Common Criteria Certification Partnership

Developer / Manufacturer

- Application for a Certification
- Advisory Services
- Issuance of a Certificate



- Evaluating the Product and the respective Documentation
- Performing Site Visits

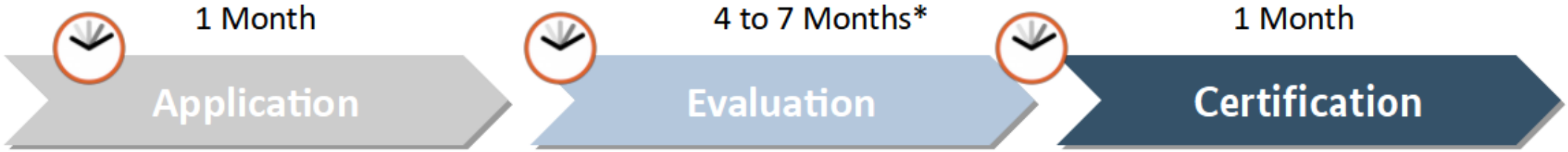
BSI Certification Body

- Evaluation Methods
- Assistance during the Evaluation
- Quality Assurance

ITSEF

Federal Office for Information Security

Common Criteria Certification – The Procedure



- Informal Advisory Services for the Developer/Manufacturer
- Formal Application Form at the Certification Body together with a Security Target and Evaluation Contract (with a concrete ITSEF)
- Planning of the procedure – Developer/Manufacturer, ITSEF and the Certification Body (**Evaluation Plan**)

- Delivery of the Product (TOE) from the side of the Developer / Manufacturer together with the documentation
- Support from the ITSEF during the evaluation process
- Evaluation support form the Certification Body and approval of the ETR (Evaluation Technical Report)

- Issuance of the Certification Report and the Certificate
- Issuance of the Certification Decision from the Certification Body
- Certificate delivery to the Developer/Manufacturer (by occasion can also take place in form of a celebration)

(*) 4 Months during a Re-Certification Procedure
7 Months during the first Certification Procedure

Federal Office
for Information Security

Fundamentals for the Common Criteria Certification Procedures

Common Criteria
(ISO/IEC 15408)

Common Evaluation Methodology
(ISO/IEC 18045)

Application Notes and
Interpretations of the Scheme (AIS)

Additional documentation:
SOG-IS MRA and CCRA MRA

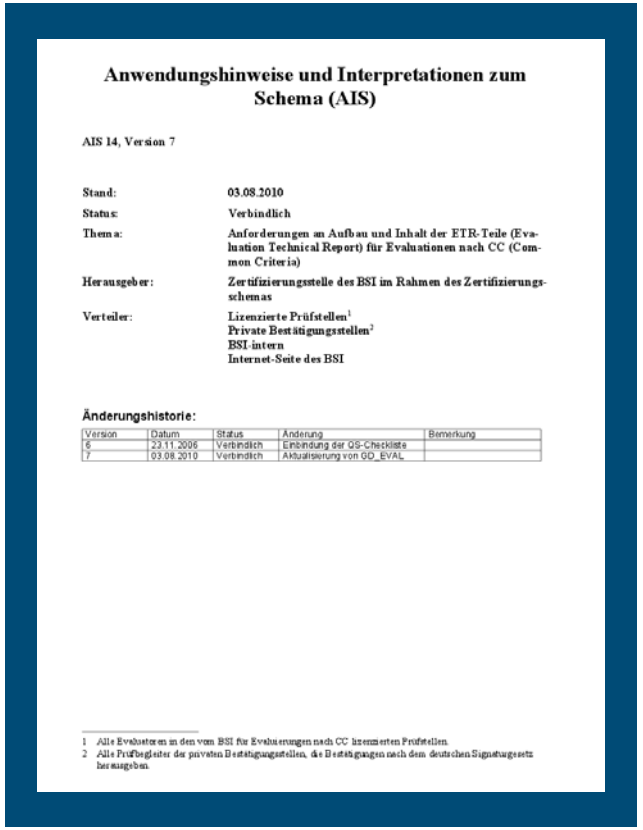
Process Descriptions (External)

- Description of process for product certification
- Requirements for applicants on the IT security certification of products, PPs and Sites

Process Descriptions (Internal)

- Product, Site and Protection Profile Certification
- ...

Application Notes and Interpretations of the Scheme (AIS)



Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS 14, Version 7

Stand:	03.08.2010
Status:	Verbindlich
Thema:	Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
Herausgeber:	Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas
Verteiler:	Lizenzierte Prüfstellen[1] Private Bestätigungsstellen[2] BSI-intern Internet-Seite des BSI

Änderungshistorie:

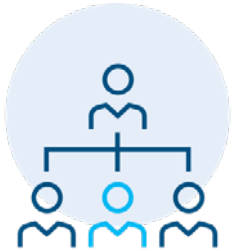
Version	Datum	Status	Änderung	Bemerkung
6	23.11.2006	Verbindlich	Einbindung der QS-Checkliste	
7	03.08.2010	Verbindlich	Aktualisierung von QD_EVAL	

1 Alle Evaluatoren in den vom BSI für Evaluierungen nach CC lizenzierten Prüfstellen.
2 Alle Prüfbegleiter der privaten Bestätigungsstellen, die Bestätigungen nach dem deutschen Signaturgesetz herausgeben.

- **AIS 14** — Requirements for the structure and the content of the single ETR-Reports
- **AIS 41** — Guidance for creation of Protection Profiles and Security Targets
- **AIS 42** — Guidance for creation of the Developer's Documentation

Additional AIS-Documents can be found here:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Anwendungshinweise-und-Interpretationen/anwendungshinweise-und-interpretationen_node.html

Mode of Operation (some excerpts)



Split of the responsibilities among certifiers and administration officers

Usage of Workflow-based system for document management

Tools for secure communication with the ITSEF and the developer

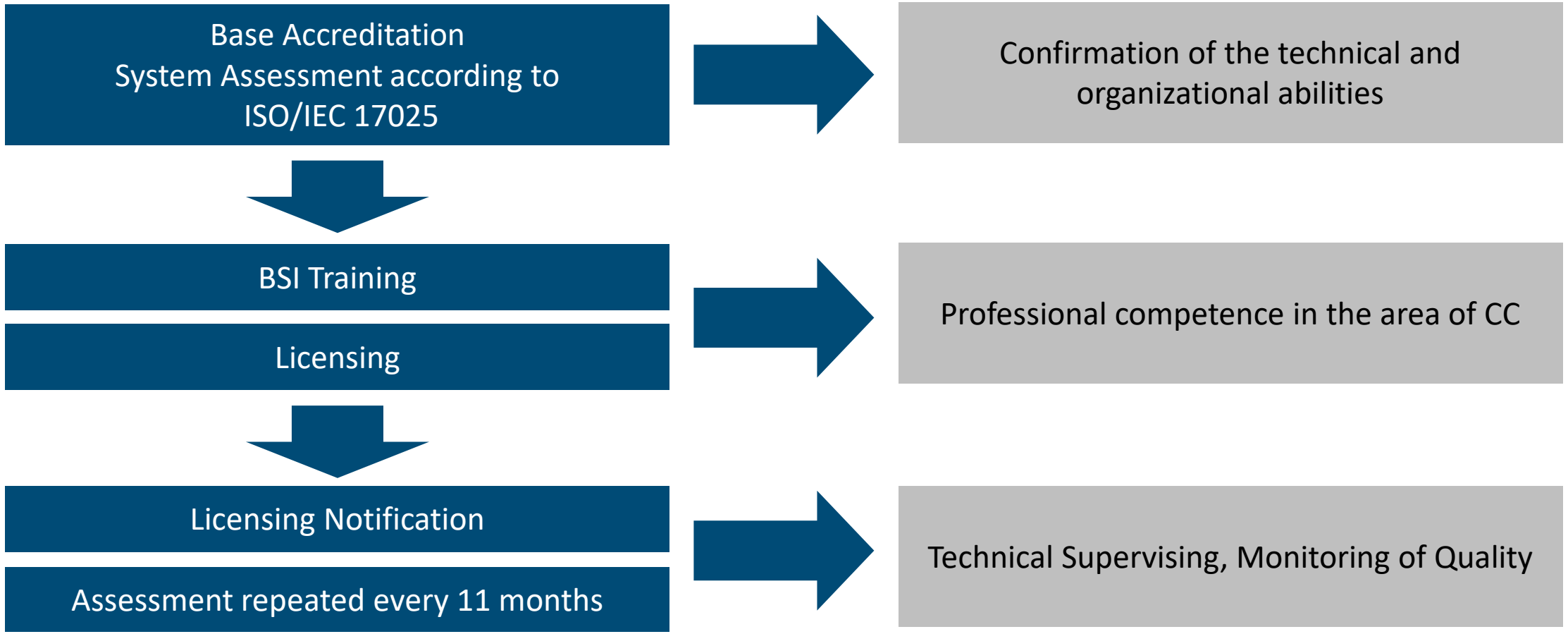
Organization and participation of workshops on specific topics, Site Visits

Regular team meetings to discuss progress and challenges in ongoing certification procedures

Some Activities of a Certifier

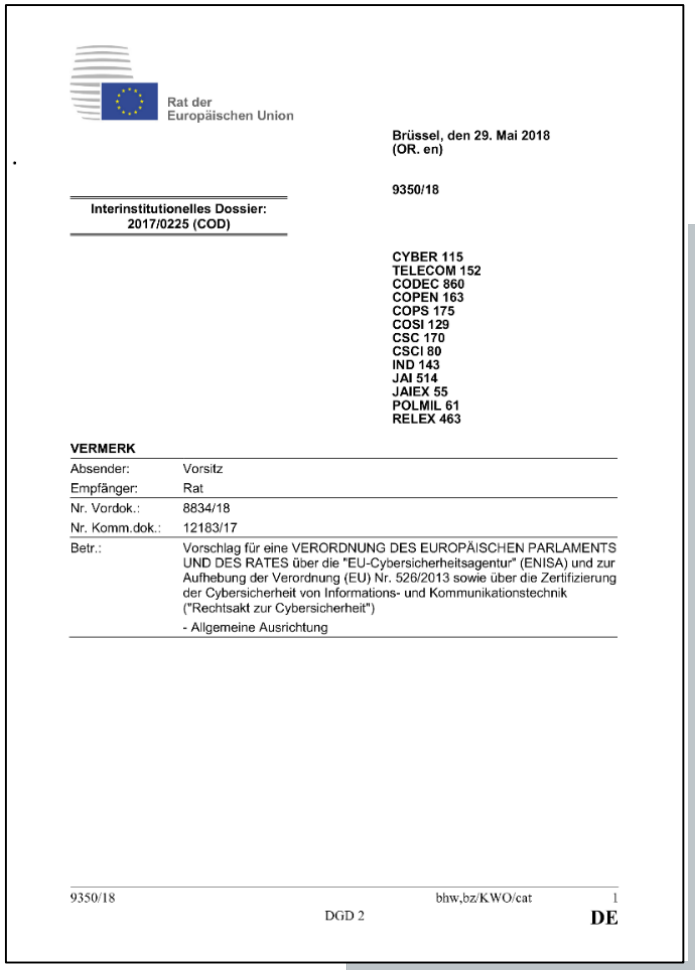
- Monitoring and feedback on Evaluation Reports, Approval of Evaluation Results
- Participating in Working Group Meetings (CCRA, SOGIS, ISO…)
- Workshops and Site Visits (in scope of a Certification Procedure)
- Preparing Certification Documentation
- Professional Trainings
- Project Management
- Advisory Services for Potential Certification Applicants
- Participation at Conferences

Licensing of ITSEFs (before CSA)



The Cybersecurity Act

- Regulation (EU) 2019/881 of 17 April 2019 = Cybersecurity Act (CSA)
- European Cybersecurity Certification Framework for IT products, services and processes
- Harmonization of existing and development of future certification schemes in EU
- Recognition of certificates in all EU member states
- Assurance Levels for certification schemes: basic, substantial and high
- National certification schemes which are covered by a European Scheme will stop operating



Rat der Europäischen Union

Brüssel, den 29. Mai 2018
(OR. en)

9350/18

Interinstitutionelles Dossier:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

VERMERK

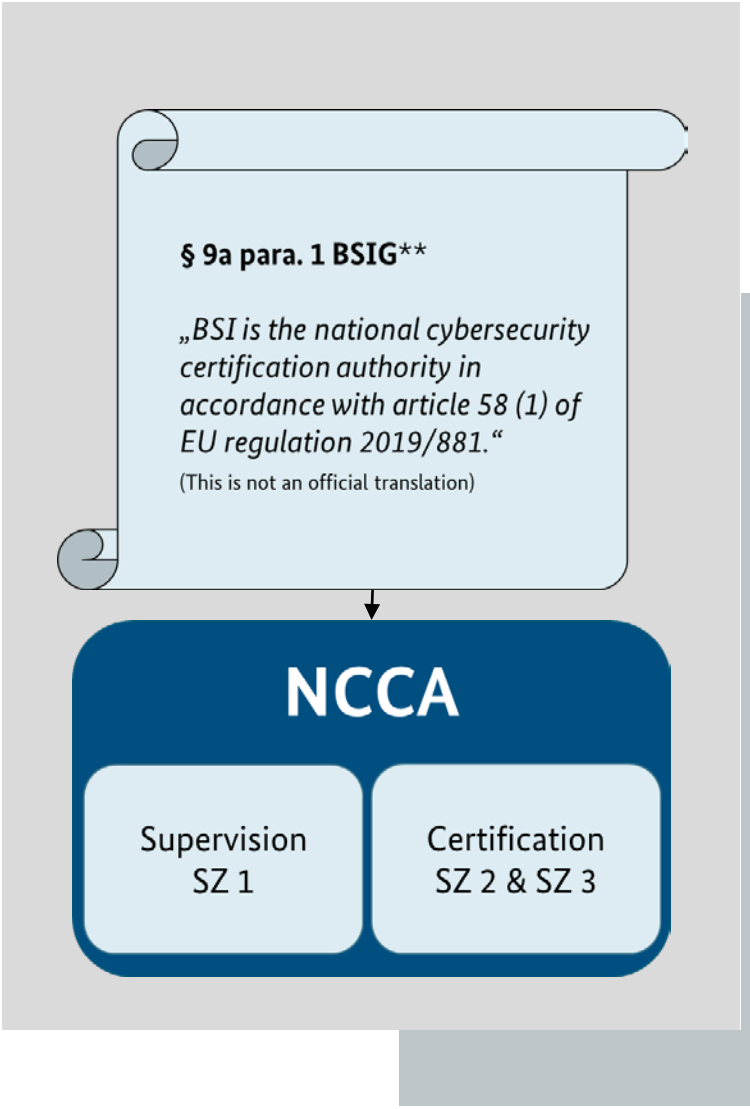
Absender:	Vorsitz
Empfänger:	Rat
Nr. Vordok.:	8834/18
Nr. Komm.dok.:	12183/17
Betr.:	Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit") - Allgemeine Ausrichtung

9350/18 bhw,bz/KWO/cat 1
DGD 2 **DE**

Federal Office for Information Security

Supervising and Certifying NCCA

- Legal Basis for the German NCCA:
  - Art. 58 if the CSA: „National Cybersecurity Certification Authority“ and the IT Security Act 2.0*
- Organizational separation to avoid personnel overlaps and conflict of interests (according to art. 58 para. 4 CSA)
- Distribution of supervising and certifying responsibilities between the three branches within division SZ
- Establishment of the necessary structures completed in 2021



Federal Office for Information Security

* Entered into force on May 28th 2021
**Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Act)

Supervising NCCA at the BSI

- Supervising and enforcing the rules of the European certification schemes
- Monitor compliance and enforce the obligations of the manufacturers or providers
- Monitor and supervise the activities of the NCCA certification authority

- Assisting & supporting the national accreditation body and authorizing CABs
- Development of the necessary structures and competences and creating awareness inside BSI for the new tasks and powers of the NCCA

- NCCA Contact: ncca@bsi.bund.de and release of NCCA-Website * and FAQ *
- Handling complaints: complaint.ncca@bsi.bund.de

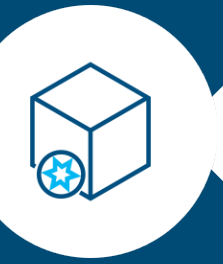
Federal Office for Information Security

*English version already published

Certifying NCCA at the BSI

- Adoption and enforcement of the rules defined by the CSA and the EUCC Scheme
- Performing certification procedures for assurance level “high“ for the EUCC scheme

- New/refined set of fundamentals for certification (EUCC Implementing Act, Supporting Documents, etc.)
- Active Participation in the groups at the EUCC Maintenance Organization



- Adaptation of the existing and establishment of new processes
- Certificate Lifecycle Management – ENISA Website

Accreditation and Authorization

- The EUCC scope of accreditation for ITSEFs (based on ISO/IEC 17025) is still under discussion
- The accreditation will be added by the authorization
- The process of authorization has to be agreed
- Applicability of ISO/IEC 17025 for CC-Evaluation ITSEFs
- BSI support during the accreditation process

Market Surveillance

- → Market Surveillance covers products under CSA as well as the German IT Security Label
- → Market Surveillance will cover occasion (event-based) related ad-hoc measures as well as standard sampling strategy based on proven methods from market surveillance
- → Starting with recruiting personal: mixed team with IT/Engineering and Public Administration background
- → Close cooperation with in-house technical experts as well as external testing facilities (likely to be ITSEFs)
- → Experience from German IT Security Label: Active Surveillance would require knowledge of the product components
- → Impulses from CRA: The Software Bill of Materials (SBOM) will play a significant role

EUCC Transition Strategy

Establishment of EUCC Transition Roadmap

Systematic identification of changes of the current CC processes and an appropriate solution; Performed by a team of senior experts within BSI including the legal department.

Adaptation of the QM System and Scheme Documentation

Systematic incorporation of changes based on the results from the EUCC Transition Roadmap including internal and external Procedure Manuals, AIS and further guidance documentation.

National CC Scheme Optimization Project

Strengthening of the German certification and evaluation infrastructure (BSI and ITSEFs) within three sub- projects: 1) "Develop workshop model process“, 2) "Specifications for reporting", 3) “Restructuring and revision of the application notes and interpretations (AIS).

Offering Best Practices for private CABs at level “substantial”

Support with providing current practices, guidance and interpretation documentation for CABs operating at the level “substantial“.

Workshops with Product Manufactures

Establishment of new format and forum for information exchange with product manufacturers starting from 14th December 2021; Presentation of the newly established structures and introduction of the substantial changes in respect to the current CC and the future EUCC processes.

Workshops with ITSEFs

Already established format for discussion and exchange with ITSEFs for scheme update and news; Until now two workshops annually with a plan to intensify the exchange and conduct a workshop every quarter of a year.

Pilots and Experimentations

Current Pilots on Accreditation and Authorization of ITSEFs and Patch Management Approach;
Further Pilots intended on integration with the ENISA Certification Website.

BSI Expertise and International Network

Bilateral exchange with the partners in the EU Member States - NCCAs, CBs and ITSEFs in terms of transitional and operational cybersecurity certification aspects.

Supporting Activities for Level “substantial”

- Involvement of CABs at level „substantial“ in the ongoing and planned activities
- Support among the concerned parties for establishment of the EUCC Infrastructure
- „Best Practice“ Exchange - Certification and Evaluation practices
- Establishment of discussion forums for knowledge transfer – national and international
- Smooth Transition and Operation under the CSA and EUCC

Important Existing Communities

EUCC Maintenance and Development

Cooperation of International Partners

Migration Support from SOGIS to EUCC

CCDB WG on EUCC/CCRA Coexistence

EUCA 2022, ICCC 2022 and other community forums

CC – Trainings
Transition to the new CC V4.0

Thank you for your attention!

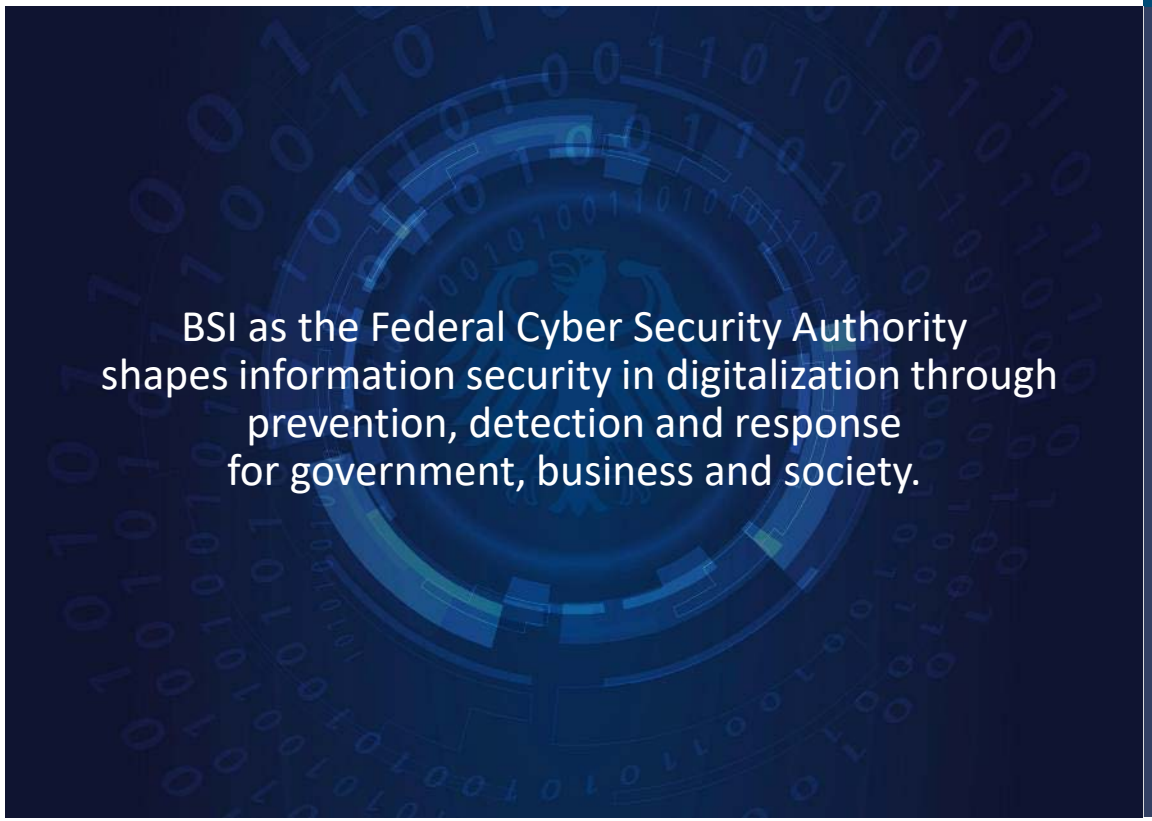
Deutschland
Digital•Sicher•BSI•

Contact

Klementina Geyer
Certifier| SZ 22 - Software Certification

klementina.geyer@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

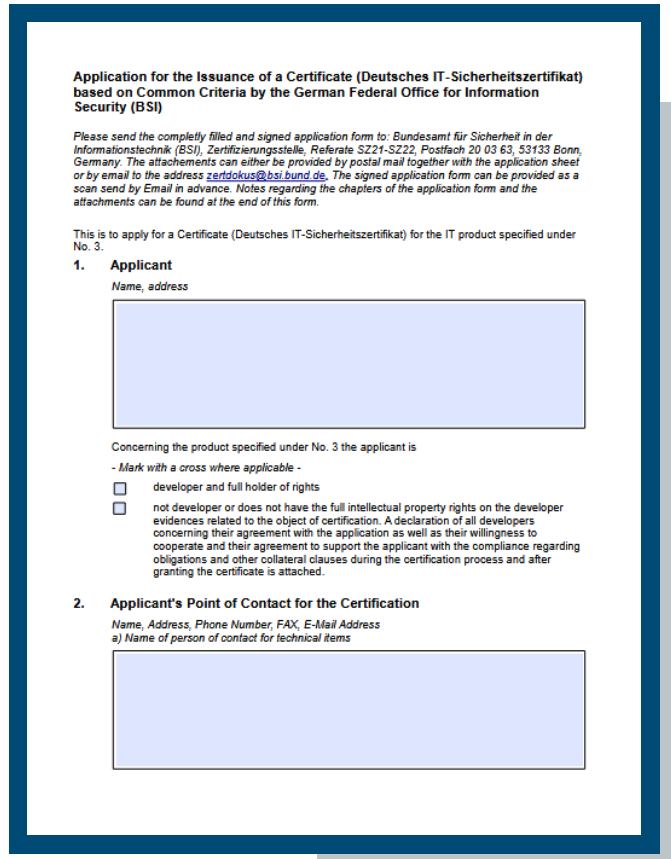


Federal Office
for Information Security

Additional Information

Application Form and Necessary Information for Certification

1. Applicant
2. Applicant Point of Contact for the Certification
3. Object of Certification
4. Evaluation Criteria
5. Type of Certification
6. Performance of the Evaluation
7. Information on already performed evaluations
8. Consulting Activities on the object of Certification and Relations
9. Announcement prior to Conclusion of the Procedure
10. Announcement upon positive Conclusion of the Procedure
11. Certification Button
12. Costs
13. Privacy
14. Additional declaration of consent and notes



Application for the Issuance of a Certificate (Deutsches IT-Sicherheitszertifikat) based on Common Criteria by the German Federal Office for Information Security (BSI)

Please send the completly filled and signed application form to: Bundesamt für Sicherheit in der Informationstechnik (BSI), Zertifizierungsstelle, Referate SZ21-SZ22, Postfach 20 03 63, 53133 Bonn, Germany. The attachements can either be provided by postal mail together with the application sheet or by email to the address zertdokus@bsi.bund.de. The signed application form can be provided as a scan send by Email in advance. Notes regarding the chapters of the application form and the attachments can be found at the end of this form.

This is to apply for a Certificate (Deutsches IT-Sicherheitszertifikat) for the IT product specified under No. 3.

1. Applicant

Name, address

Concerning the product specified under No. 3 the applicant is

- Mark with a cross where applicable -

☐ developer and full holder of rights

☐ not developer or does not have the full intellectual property rights on the developer evidences related to the object of certification. A declaration of all developers concerning their agreement with the application as well as their willingness to cooperate and their agreement to support the applicant with the compliance regarding obligations and other collateral clauses during the certification process and after granting the certificate is attached.

2. Applicant's Point of Contact for the Certification

Name, Address, Phone Number, FAX, E-Mail Address
a) Name of person of contact for technical items

Federal Office
for Information Security

Evaluation Plan and Necessary Information

Requirements for the Evaluation Plan defined in the Certification Programs:

- Evaluation Basis (criteria and methodology, applicable AIS, relevant governmental laws..)
- TOE Evaluation Description (security functionality, tasks of the ITSEF, personnel assignment…)
- Competence of the ITSEFs and the assigned personnel
- Tools used for the evaluation tasks
- Detailed Evaluation Work Plan (definition of work packages, site visits if included, testing approach...)
- Other information (language of developer information, exchange of information…)

Requirements on Single Evaluation Reports

Specified in AIS 14 – Guidelines on Evaluation Reports:

- ETR-Part ASE
- ETR-Part ADV
- ETR-Part ADV_AGD
- ETR-Part ALC
- ETR-Part ATE
- ETR-Part AVA

Requirements on Evaluation Technical Report (ETR)

Specified in AIS 19 – Requirements on the content and structure of the ETR:

- Evaluation Background Information (TOE description, involved persons, deadlines, evaluation approach)
- TOE Scope of Delivery
- Evaluated Configuration (exact description of the TOE Configuration, Test Configuration, Development and Production Sites, Cryptographic Functionalities)
- Architectural Description
- Vulnerabilities
- Requirements for the Usage of the Evaluated Product
- Final Verdict of the Evaluation Body

Preparation of the Certification Documentation

- Certificate
- Certification Report
- Official Hearing (conditions for validity of the certificate)
- Certification Notification (conditions for validity of the certificate)
- Publication of the Certificate, Certification Report and ST on the BSI website
- Providing Certification Button (EUCC: Certification Label) (including terms and conditions for usage)

Types of Certification Processes

- Initial Certification
- Re-Certification: a re-certification is a process of assurance in case of a so-called major change (security relevant changes)
- Maintenance: maintenance is a process of assurance in case of a so-called minor change (security irrelevant changes). The decision if a specific change is a major or minor change is made by the certification body as a result of an assessment of the evidence provided
- Re-assessment: change in the threat environment - update of the vulnerability analysis of the product
- EUCC: Scope Reduction, Patch Management (in progress)

European Cooperation: The SOGIS-MRA

Consuming and certifying nations (generally up to EAL4, for Technical Domains up to EAL7)

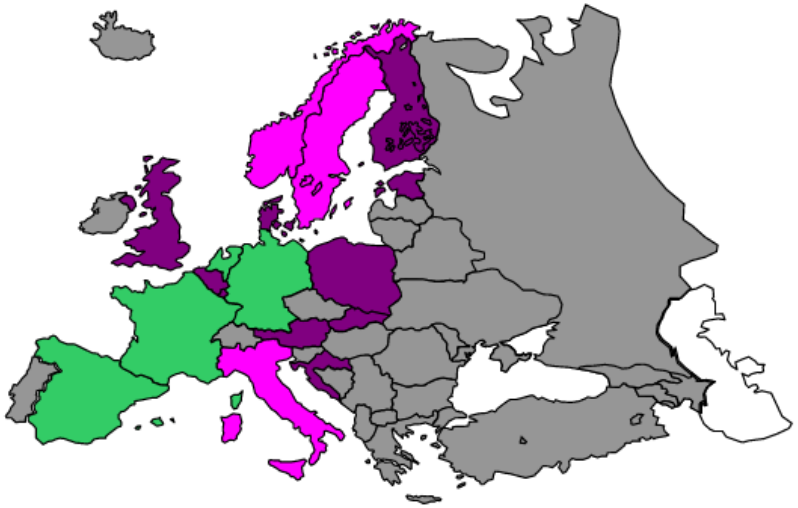
- Germany
- France
- Netherlands
- Spain

Consuming and certifying nations (up to EAL4)

- Italy
- Norway
- Sweden

Consuming nations

- UK
- Belgium
- Denmark
- Estonia
- Finland
- Croatia
- Luxembourg
- Austria
- Poland
- Slovakia



International Recognition of Certificates under CCRA

Certifying Nations

- Australia & New Zealand
- Netherlands
- Canada
- Singapore
- USA
- Germany
- Italy
- Japan
- France
- Spain
- South Korea
- Norway
- Sweden
- Turkey
- Malaysia
- India

- generally: up to EAL2
- Possibly up to EAL4 based on cPPs

Recognising Nations

- Finland
- Greece
- Hungary
- Denmark
- Austria
- Israel
- Ethiopia
- Qatar
- Indonesia
- Pakistan
- Poland
- United Kingdom
- Czech Rep.
- Slovak Rep.

https://www.commoncriteriaportal.org

DISCUSSION

Federal Office
for Information Security

How to operate as a Certification Body in context of systems

Agenda

1. Information security and motivation
2. The BSI standards & publications
3. IT-GS certification
4. Advantages of certification
5. Other

01

Information security and motivation

GettyImages - © Andrezej Wojcicki - Science Photo Library

Federal Office
for Information Security

Information security

- Information security aims to protect information.
- The basic values of information security include availability, confidentiality and integrity of information.
- Information can be stored on paper, in IT systems or even in heads

- **Information security delivers more than just IT security**
- **Information security must be managed → Information security management system (ISMS)**

Security is...

- ... no product!
  - You cannot buy security
  - Security must be created
  - Of course, you can also use existing products for this purpose
- ... not a project!
  - It is not enough to create security once
  - Security must be maintained
- ... a process!
- ... management issue!

IT-Grundschutz

IT-Grundschutz pursues a holistic approach

- Standard level of security to protect business-relevant information for infrastructural, organisational, personnel and technical security
- Higher-level security requirements are provided, which are necessary for sensitive areas.

APP.5.3 General E-Mail Clients and Servers

1 Description

1.1 Introduction

E-mail is one of the oldest and commonly used Internet applications. E-mails are used to send text and attached files to other people. Users require an e-mail address for this purpose.

E-mail applications require e-mail servers that can send and receive electronic messages. As a rule, e-mail clients retrieve messages intended for them from an e-mail server using the POP3 or IMAP protocols and send messages to the e-mail server using the SMTP protocol, which forwards them to another e-mail server if necessary.

Since e-mail is widely used, especially at companies and public authorities, e-mail servers are often targeted by attackers.

E-mail clients are also the focus of attacks, including those that attempt to deliver malware via e-mail. In addition, e-mails are often used as a tool for social engineering attacks.

For these reasons, the secure operation and use of e-mail applications is of particular importance.

1.2 Objective

The objective of this module is to protect information that is processed with e-mail clients or on e-mail servers.

1.3 Not in scope and modelling

The module APP.5.3 *General E-Mail Clients and Servers* must be applied to each e-mail client and server in the information domain under consideration.

The module includes requirements for general e-mail servers and clients. Requirements for server platforms, operating systems, and clients are not covered. These can be found in the modules SYS.1.1 *General Server* and SYS.2.1 *General Client*, as well as in the respective operating-system-specific modules.

Within the context of an information domain, the module APP.5.3 *General E-Mail Clients and Servers* is mostly used in combination with another specific module of layer APP.5 *E-Mail / Groupware / Communication*. These must also be implemented separately. Among others, these modules include APP.5.2 *Microsoft Exchange and Outlook*.

Modules GS-Kompendium Document structure

- Length: approx. 10 pages!
- Description
  - Introduction, objective, delimitation
- Specific threat situation
- Requirements
  - Basic requirements
  - Standard requirements
  - Requirements for increased need of protection
- References to further information
- Appendix: Cross-reference table
- Supplementary: Implementation instructions with concrete measures

02

The BSI standards and publications

GettyImages - © Ralf Hiemisch

IT-Grundschutz Publications

- IT-Grundschutz compendium in various formats
- Implementation notes for the IT-Grundschutz Compendium
- Checklists
- Cross-reference tables
- BSI standards 200-1, 200-2, 200-3, 100-4 (200-4 in progress)
- IT-GS Profiles

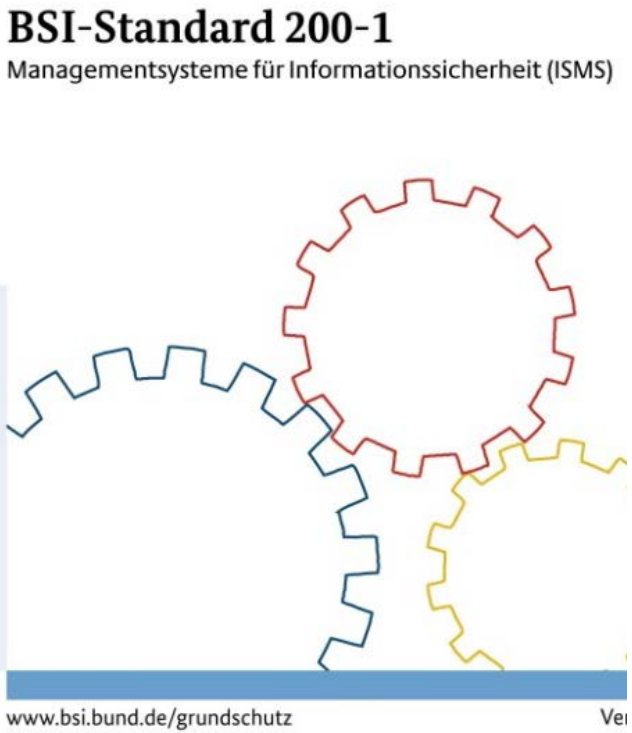
- All available **free of charge** online at https://www.bsi.bund.de/grundschutz

BSI Standard 200-1
Information Security Management Systems

- Defines general requirements for an Information Security Management System (ISMS)

- Target group: Management
- Compatible with ISO/IEC 27001
- Interpretation of the standard

Federal Office
for Information Security



BSI Standard 200-1
Answers to the following questions

- What are the success factors in managing information security?
- How can the security process be controlled and monitored by the responsible management?
- How are security objectives and an appropriate security strategy developed?
- How are security measures selected and security concepts drawn up?
- How can a level of security once achieved be permanently maintained and improved?

BSI Standard 200-2
IT-Grundschutz-Methodology

- Describes the concrete procedures for setting up an ISMS. Also offers procedures for getting started and concrete examples based on a fictitious company (Recplast GmbH).

- Target group: Information Security Officers (ISB)
- Compatible with ISO/IEC 2700X

Federal Office
for Information Security

BSI Standard 200-3
Risk Analysis based on IT-Grundschutz

- Bundling and description of all risk-related work steps, such as the implementation of a risk decision process.

- Target group: Information Security Officers (ISB)
- Compatible with ISO/IEC 2700X

Federal Office
for Information Security

Bundesamt
für Sicherheit in der
Informationstechnik

BSI Standard 100-4
Business Continuity Management

- Systematic description of how to set up Business Continuity Management in a public authority or a company.

- Target group: Information Security Officers (ISB)
- Compatible with ISO/IEC 2700X

Federal Office
for Information Security

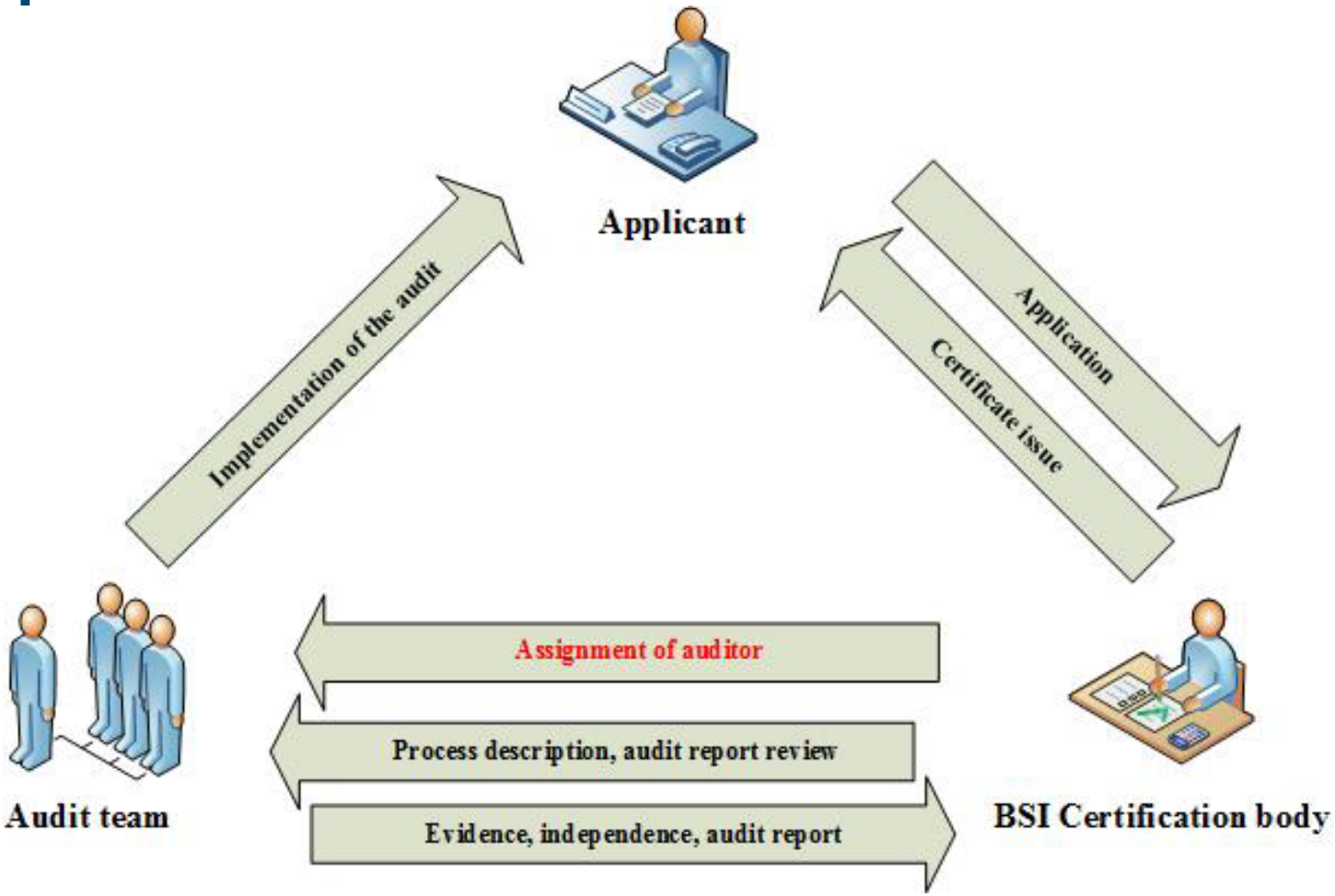
IT-Grundschutz profiles
Overview

- Tool for user-specific recommendations
- Individual adaptations of the IT-Grundschutz to the respective needs possible
- Considers opportunities and risks of the institution
- Profiles refer to typical IT scenarios
- Profiles are usually created by third parties (associations, industries, ...) and not by the BSI
- Not to be understood as a BSI requirement!

03

IT-GS certification

Allocation of roles within the Certification process



Federal Office
for Information Security

BSI Certification Body - roles

- **Unit SZ 25**
  Certification body – consisting of 3 persons

- **Unit SZ 13**
  Test support – consisting of 4 persons

- **IT-Grundschutz CertLabs**
  2 CertLabs which test IT-Grundschutz procedures on behalf of the BSI

BSI Certification Body – numbers & facts

- **Certification body exists since 2002**
- **501** total ISO 27001 certificates on the basis of IT-Grundschutz
- **136** Currently valid ISO 27001 certificates issued on the basis of IT-Grundschutz
  49% Business vs. 51% Government

Certification-relevant documentation

- **Auditing scheme**

  The addressees here are primarily the auditors

- **Certification scheme**

  The addressees here are both, the auditors and the applicants or certificate holders

- **Person Certification: Program auditors or audit team leaders**

  Targets persons who would like to work as certified ISO 27001 auditors for audits based on IT-Grundschutz

Auditing

- The basic procedure and requirements for ISO 27001 certification based on IT-Grundschutz are described in the **certification scheme**
- The **audit scheme** describes the requirements for the audit action of the audit team leader and the members of the audit team
- This includes an overview of the audit and certification process, professional ethics and a detailed description of the individual audit types and phases.

Initial-Certification

- The procedure is opened with the acceptance of the application by the BSI certification body
  - Pre-audit possible
- Document check of the submitted reference documents by audit team
- On-site implementation audit (random sampling) by audit team
- => Audit report
- Acceptance of audit report by BSI

Monitoring audit

- No renewed application necessary, part of the initial / Re-certification
- 1 and 2 years after issuance of the certificate
- No reissue of the certificate
- Unscheduled surveillance audits, e.g. for the purpose of
  - Verification of the correction of serious deviations

Re-Certification

- original object of investigation has not fundamentally changed
- Review of reference documents at the earliest 4 months before expiry of certification
- Procedure comparable with initial certification
  - Reference to expiring certificate must be made (e.g. explanation of module selection, changes).

05

EUCS

GettyImages - © enjoynz

Federal Office
for Information Security

EUCS Status

- BSI will be CAB for EUCS if a scheme for „high“ is implemented
- **Requirements for conformity assessment bodies certifying cloud services** under development in JTC 13
- Follows the general requirements of ISO/IEC 17065:2012 with a focus on processes and services rather than products
- Evaluation types are inspection, testing, **audit**, verification and validation

Evaluations

- Stage 1
  - Preparation and planning,
  - ressource allocation,
  - evaluation of evidence

- Stage 2
  - Evidence of controls are in accordance to their design
  - Check validity of documentation on-site or remote
  - Issuing the evaluation report

Contact

Deutschland
Digital•Sicher•BSI•

BSI Unit SZ 25

ISO 27001 certification based on IT-Grundschutz :

gs-zert@bsi.bund.de
Federal Office for Information Security
Unit SZ25
PO Box 20 03 63
53133 Bonn

Time for your questions

Federal Office
for Information Security

DISCUSSION

60 min

RED ALERT LABS
IoT Security

Workshop

How to build and operate testing laboratory (ITSEF) in the context of the EUCC

02/11/2022

RED ALERT LABS

RED ALERT LABS
IoT Security

Our Services

SECURITY CONSULTING

- Risk Assessment
- Secure Design
- Certification Schemes
- Strategic plan

SECURITY EVALUATION

- Pentesting
- Regulations
- Standards
- Certification

SECURITY INNOVATION

- Risks Analysis
- Product Assessment
- Trusted Procurement
- Vulnerability Management

SECURITY TRAINING

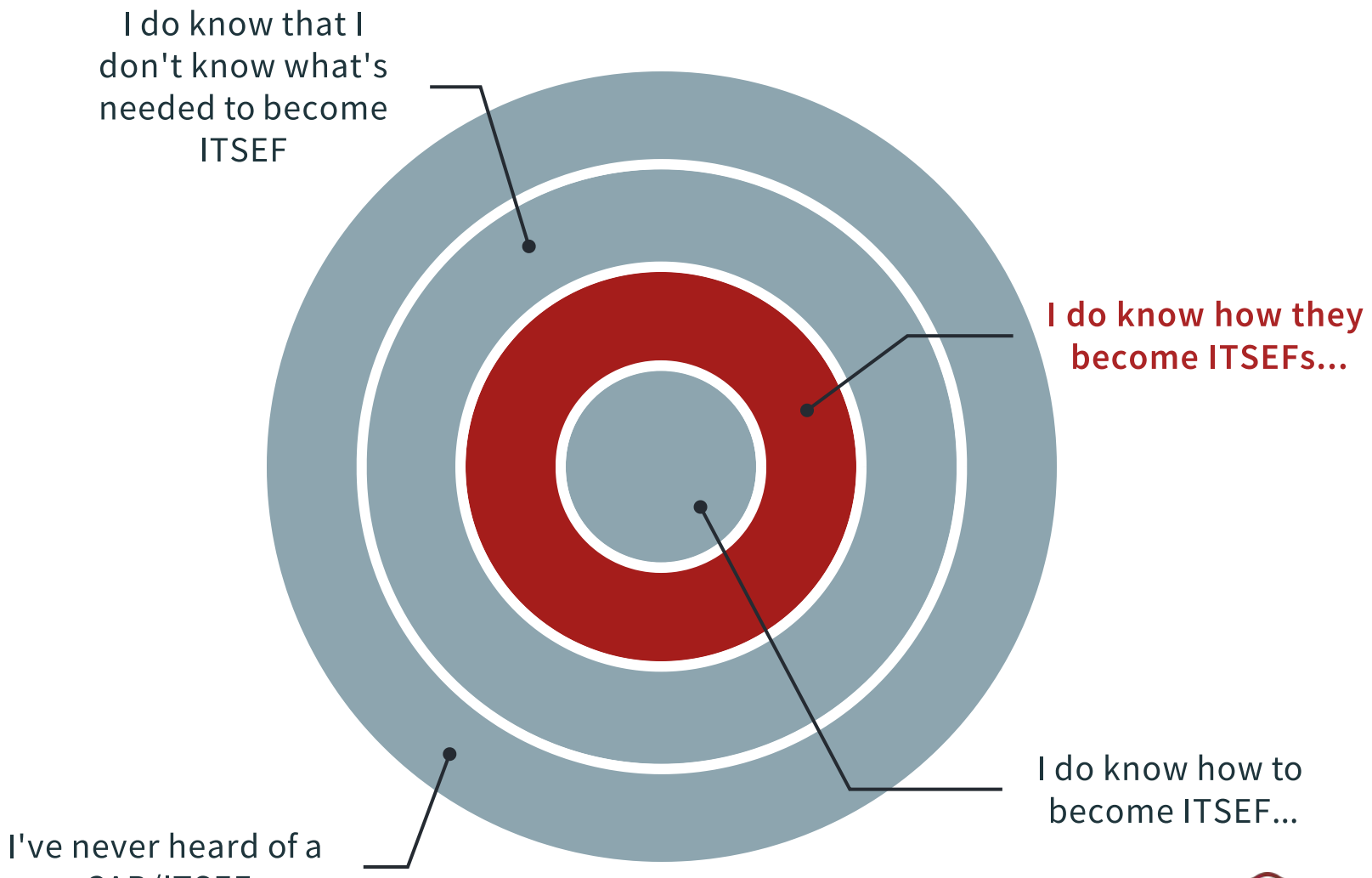
- Cybersecurity Act
- Certification Schemes
- Common Criteria
- IoT Cybersecurity
- Cyber Resillience Act

RED ALERT LABS
IoT Security

Road towards becoming an ITSEF

RED ALERT LABS
IoT Security

OUR SESSION GOAL



RED ALERT LABS
IoT Security

#1 DEFINE STRATEGIC GOALS

market, level of assurance, scope, key results, short long term, …

RED ALERT LABS
IoT Security

Strategic Projection

- **Business Objectives**
  Realistic objectives and Key Results (short, mid, long-term)
- **Structure and Governance**
  Dependent, Independent, Consulting vs Evaluation
- **Budgeting**
  How much money should I be spending ?
- **Market study**
- **Schemes positioning**
  ICT product ? processes ? services? what are my options ? Mandatory ? Voluntary ? Regulations ?
- **Competitive Landscape**
  Locally and on the EU level
- **Assurance Level**
  From Substantial to High
- **Level of maturity, skills and capacities**

https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study
https://www.enisa.europa.eu/events/cybersecurity-market-conference

RED ALERT LABS
IoT Security

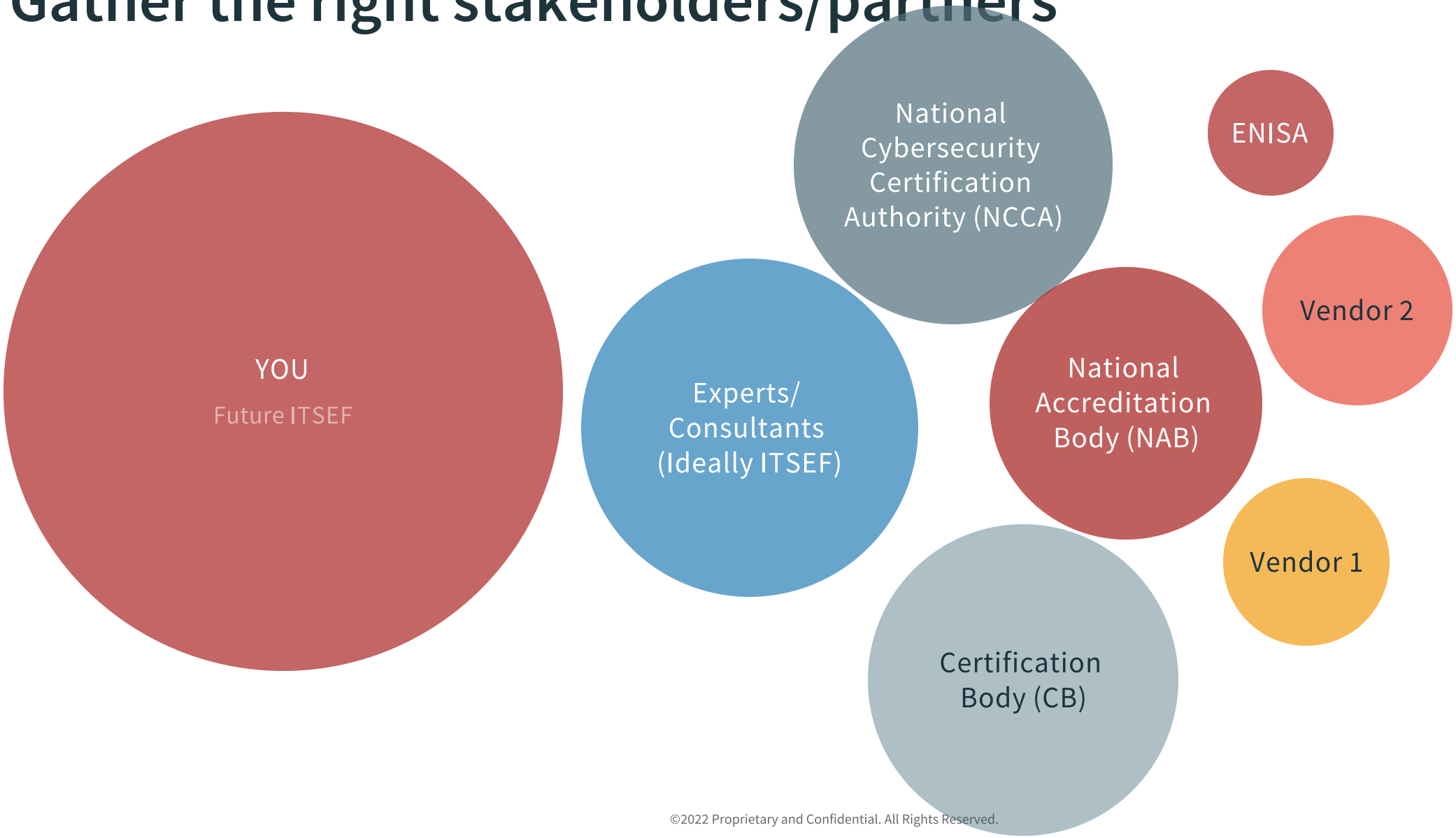
#2 BUILD A CONSORTIUM

Stakeholders, Experts, CABs, liaison, ...

RED ALERT LABS
IoT Security

The Consortium (ideally)

Gather the right stakeholders/partners



RED ALERT LABS
IoT Security

From Design to Certification

Coordinate Goals

1 | APPLICANT

VENDOR 1

VENDOR 1 has developed an ICT product with security features and they identified the need to certify it under the CC/EUCC scheme.

2 | WHICH CAB ?

CB

VENDOR 1 team submitted their certification application to the CB.

3 | HOW CAN I GET ACCREDITED ?

ITSEF

ITSEF requested an accreditation by the NAB and an AUTHORISATION/NOTIFICATION by NCCA

4 | HOW TO GET READY ?

VENDOR 1

Vendor 1 prepares the evidence supported by CC consultants

5 | HOW TO EVALUATE and CERTIFY ?

ITSEF, CB

The CAB runs the evaluation process, deliver a report and issue a certificate

6 | HOW DO I UPDATE MY CERTIFICATE ?

VENDOR 1 requested an update to its certificate due to an update of his product following a vulnerability disclosure, should I inform ENISA ?

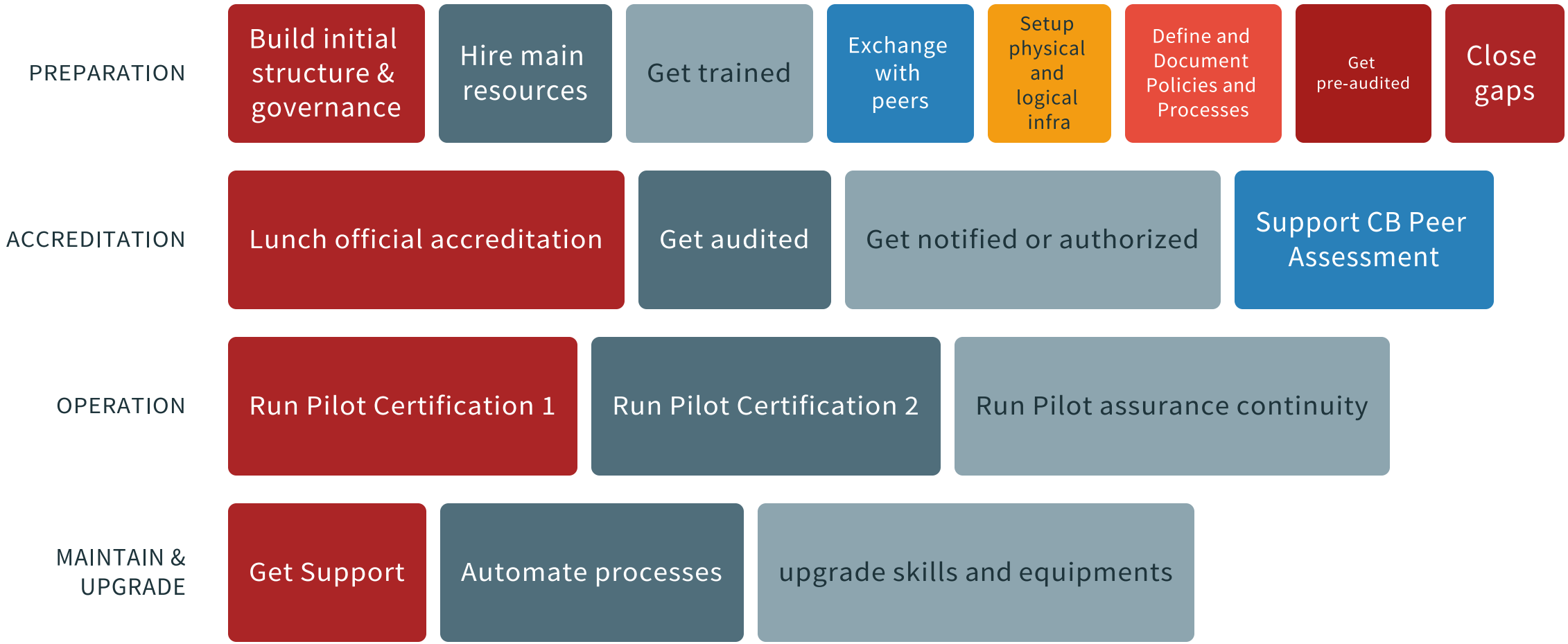
RED ALERT LABS
IoT Security

#3 CREATE A PROJECT

prio, activities, timeline, ...

RED ALERT LABS
IoT Security

Project Planning



RED ALERT LABS
IoT Security

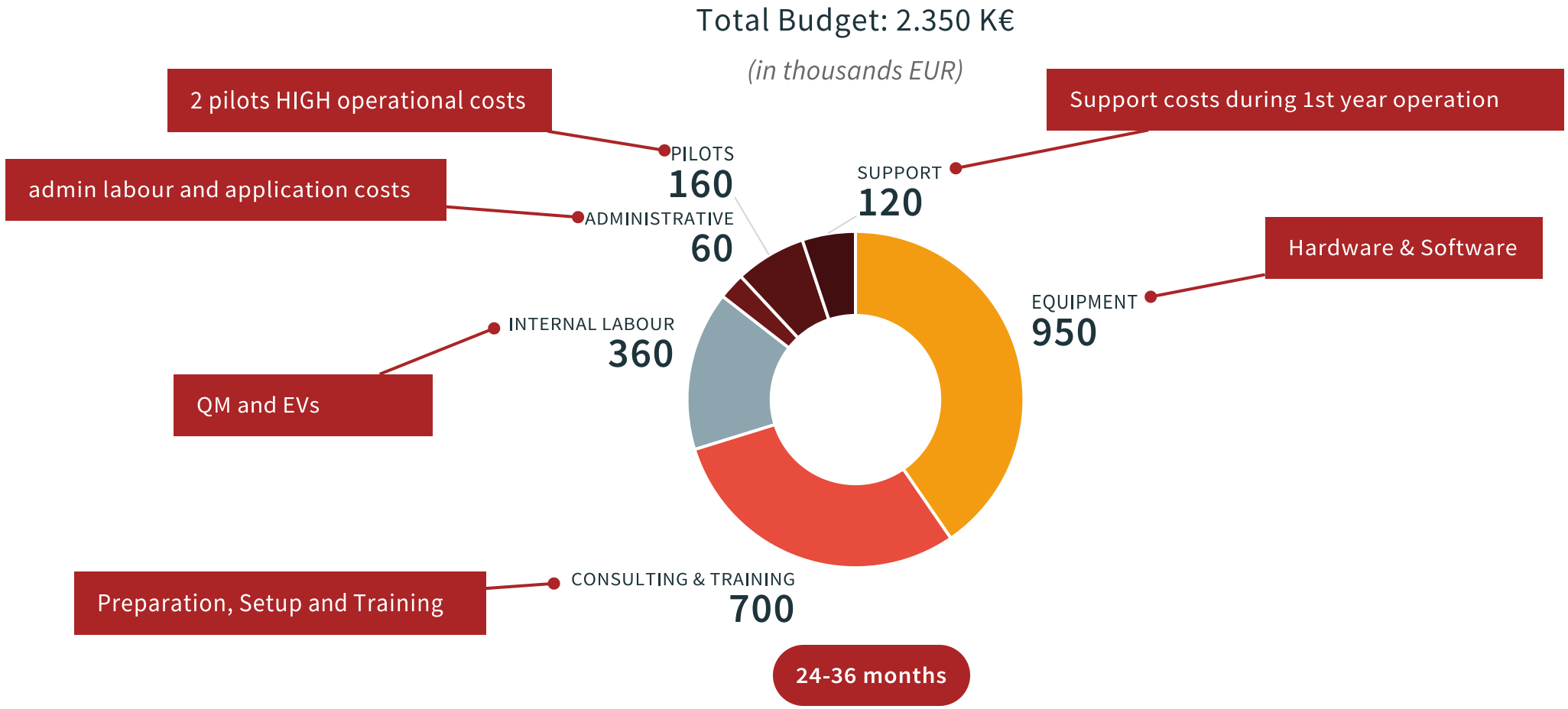
#4 EFFORT & COSTS

estimation, budgeting

RED ALERT LABS
IoT Security

Budget Rough Estimation

EUCC level **HIGH** (EAL 4+ / AVA_VAN.5)



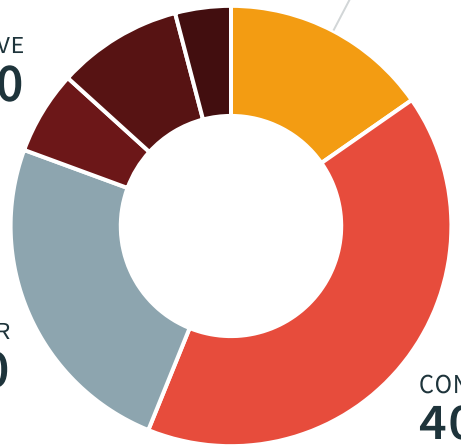
RED ALERT LABS
IoT Security

Budget Rough Estimation

EUCC level **SUBSTANTIAL** (EAL 2-3 / AVA_VAN.2)

Total Budget: 980 K€

(in thousands EUR)



2 pilots SUBSTANTIAL operational costs

admin labour and application costs

QM and EVs

Support costs during 1st year operation

Hardware & Software

Preparation, Setup and Training

18-30 months

RED ALERT LABS
IoT Security

#5 SEEK FUNDING

Grants, Investors, Customers, etc.

RED ALERT LABS
IoT Security

Cybersecurity and Trust (DIGITAL-ECCC-2022-CYBER-03)

Capacity Building

Strengthen NCCAs, CABs and NABs. exchange of best practices and staff trainings; deploy innovative evaluation methods for ICT Products

Testing Capabilities

Improve the cybersecurity and interoperability testing capabilities in all Member States, including in the area of 5G solutions.

Support SMEs

Support SMEs to audit their infrastructure in view of improving their cybersecurity protection.

Standardisation Actions

(e.g. creation of protection profiles or adoption/improvement of standards used in certification schemes)

RED ALERT LABS
IoT Security

Quick Highlights

TEST-CERT-CAPABILITIES

Planned opening date

15 November 2022

Deadline for Submission

15 February 2023 17:00:00 Brussels time

Total Budget

5M€

Next Steps

Build a consortium, complete and submit proposal

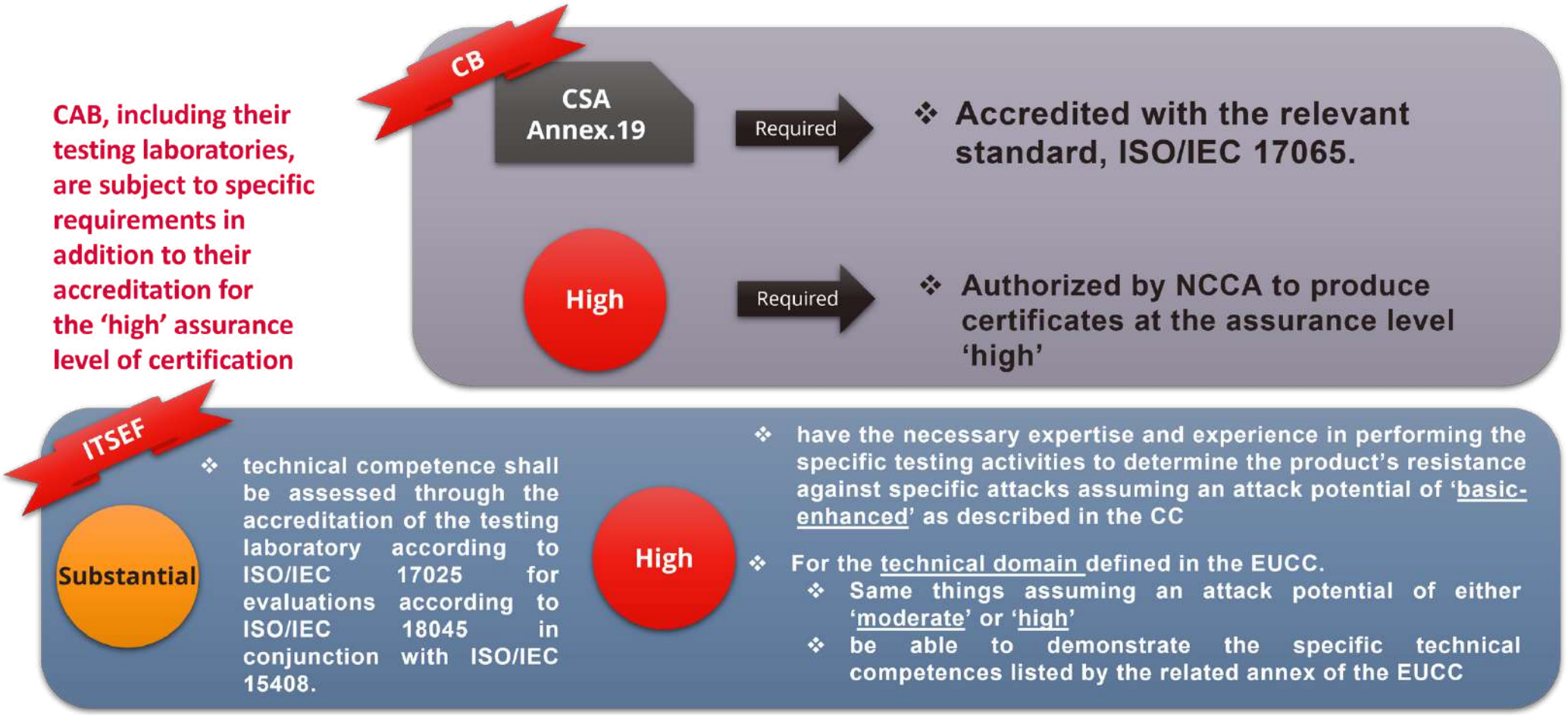
RED ALERT LABS
IoT Security

#6 START BUILDING

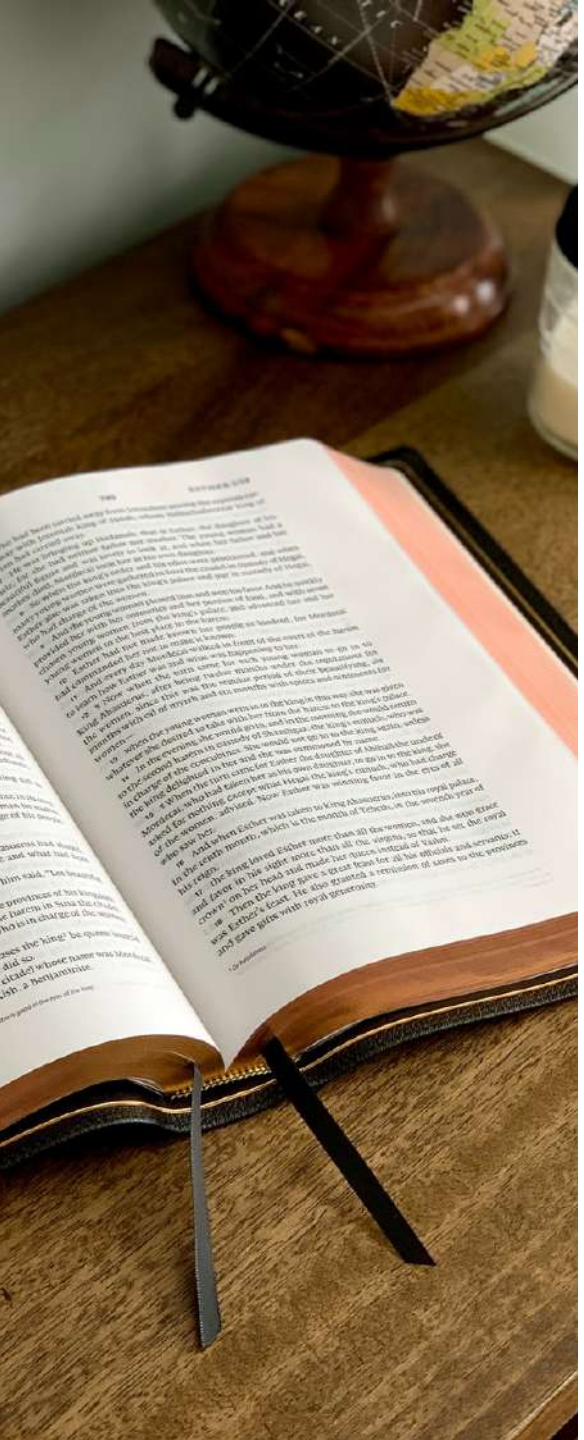
framework, resources, trainings, infra, docs,

RED ALERT LABS
IoT Security

Requirement applicable to CAB



Understanding the CSA, Standards and Additional Requirements



CSA Reminder

Application of international standards to the accreditation of ITSEFs.

The Cybersecurity Act prescribes the obligation

that **schemes refer to** international, European or national **standards** that are to be applied in the evaluation or, where such standards are not available **or** appropriate, **to technical specifications** that **meet the requirements set out in Annex II to Regulation (EU) No 1025/2012** or, if such specifications are not available, to technical specifications **or other cybersecurity requirements defined in the European cybersecurity certification scheme**.

In this respect it should be taken into account that the following standards are applicable to the accreditation of ITSEFs

- ISO/IEC 17025:2017
- ISO/IEC TS 23532-1:2021

  Inside it, references to “scheme owner(s)” should be understood in this context as referring to the related CB and NCCA.
- ISO/IEC 19896. (Part 1 & 3)
- EUCC
- Additional requirements

RED ALERT LABS
IoT Security

Example of general accreditation requirements from the CSA

Annex - REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

10.	At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services or ICT processes, a conformity assessment body shall have at its disposal the necessary: - (a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; - (b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. [...] - (c) procedures for the performance of activities [...]	ISO/IEC 17025:2017, 6.2 ISO/IEC 17025:2017, 7.2

RED ALERT LABS
IoT Security

Example of general accreditation requirements from the CSA

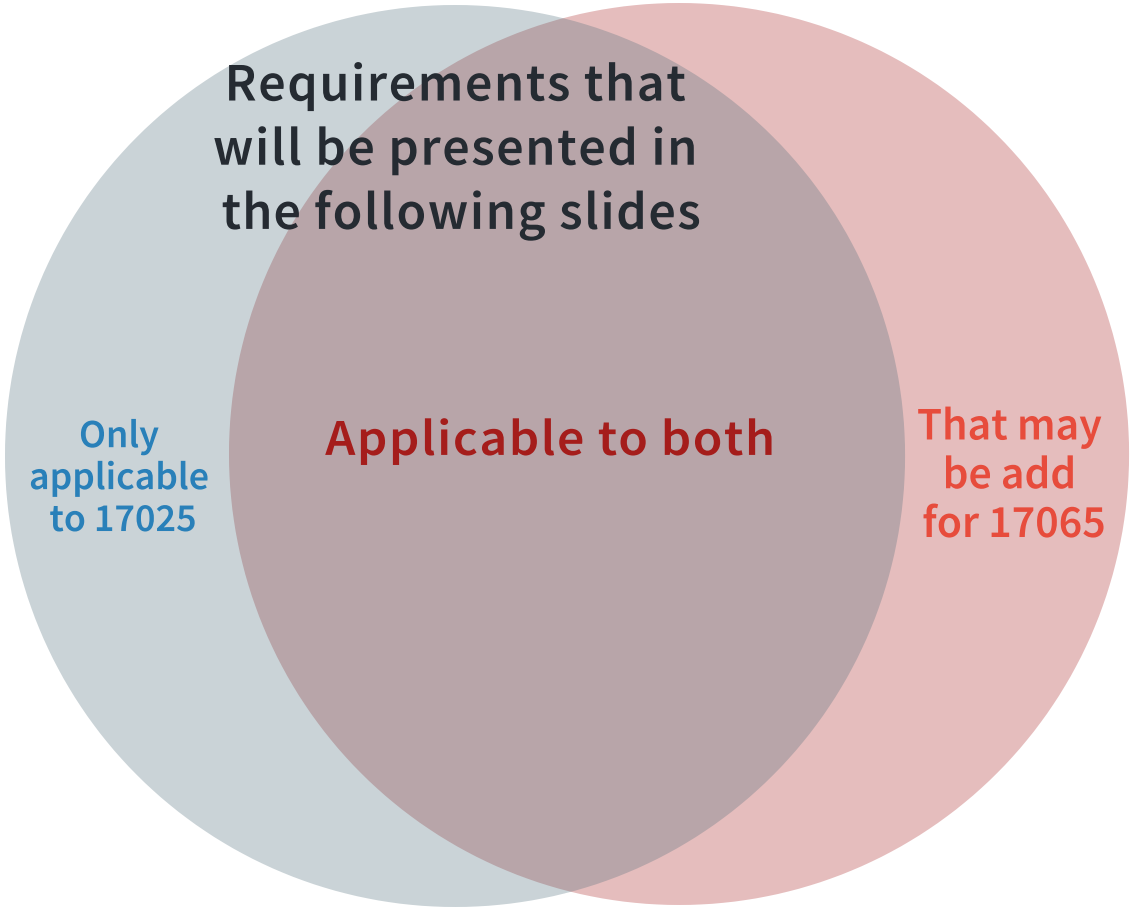
Annex - REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

18.	Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.	
19.	Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.	
20.	Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.	next slides

RED ALERT LABS
IoT Security

Additional requirements.

In addition to the requirements included in ISO/IEC 17025:2017 and ISO/IEC TS 23532-1:2021, the following requirements apply to the accreditation of an EUCC ITSEF.



The majority of the requirements are as applicable to CB as they are for the ITSEF

Impartiality Example

Reminder ISO 17025

Impartiality Example

Addition to ISO/IEC 17025:2017, 4.1

- Generic training

  Generic training (from a public list of pre-established training) **with safeguards on trainings carried out in-house for a single company** (generic training with adaptation deletion/addition of a part, no case studies from the party, no workshop demonstration) **shall not be considered consultancy**.

- Bespoke training

  Bespoke training on the party's specific activities is not allowed.

RED ALERT LABS
IoT Security

Confidentiality Example

Reminder ISO 17025

- The certification body is legally responsible for information generated during its activities
- The certification body must inform customer of any confidential information to be divulged.
- Customer information obtained from other sources must be kept confidential
- Identity of such a source must not be shared with customer
- Personnel must keep all information obtained during CB activities confidential except as required by law

Other categories are also subject to these additional requirements

Addition to ISO/IEC TS 23532-1:2021, 4.2.8

- Proprietary Information protection

  Examples: **personal data** covering GDPR, information necessary for the **implementation** of **EUCC**, **handling** of publicly unknown and subsequently detected **vulnerabilities**

- Examples of measures

  e.g The information system shall include **tools** that provide **encryption functionalities** for non-public Information at rest. These tools should be **referenced by an ENISA** or a **National guidance document.**

  e.g **Secure electronic storage and communication** must be achieved for non-public Information **through standard cryptographic methods and algorithms.** The ITSEF shall refer to **and comply with ENISA or National cryptography guidelines for** further guidance.

- Evaluation contracts between ITSEFs and their customers

  e.g identify which parties will have access to the evaluation evidence and findings that are part of the certification process,

  e.g. inform CB about contract obligations

RED ALERT LABS
IoT Security

Competences Example

Reminder ISO 17025

Personnel, internal or external, must act impartially.

Labs must document the competence requirement of each function that influences lab results.

Personnel must have the required competence for their job description.

Management must communicate to personnel their duties, responsibilities and authorisation.

Labs must retain records

- determining the competency requirements ;
- supervision of personnel ;
- authorization of personnel.

Labs must also authorize personnel

- Development, modification, verification, and validation of methods ;
- Analysis of results ;
- Reports, reviews and authorization of results.

Competences Example

EUCC, “6. SPECIFIC REQUIREMENTS APPLICABLE TO A CAB”
ISO/IEC 17025:2017, ”6.2 Personnel”

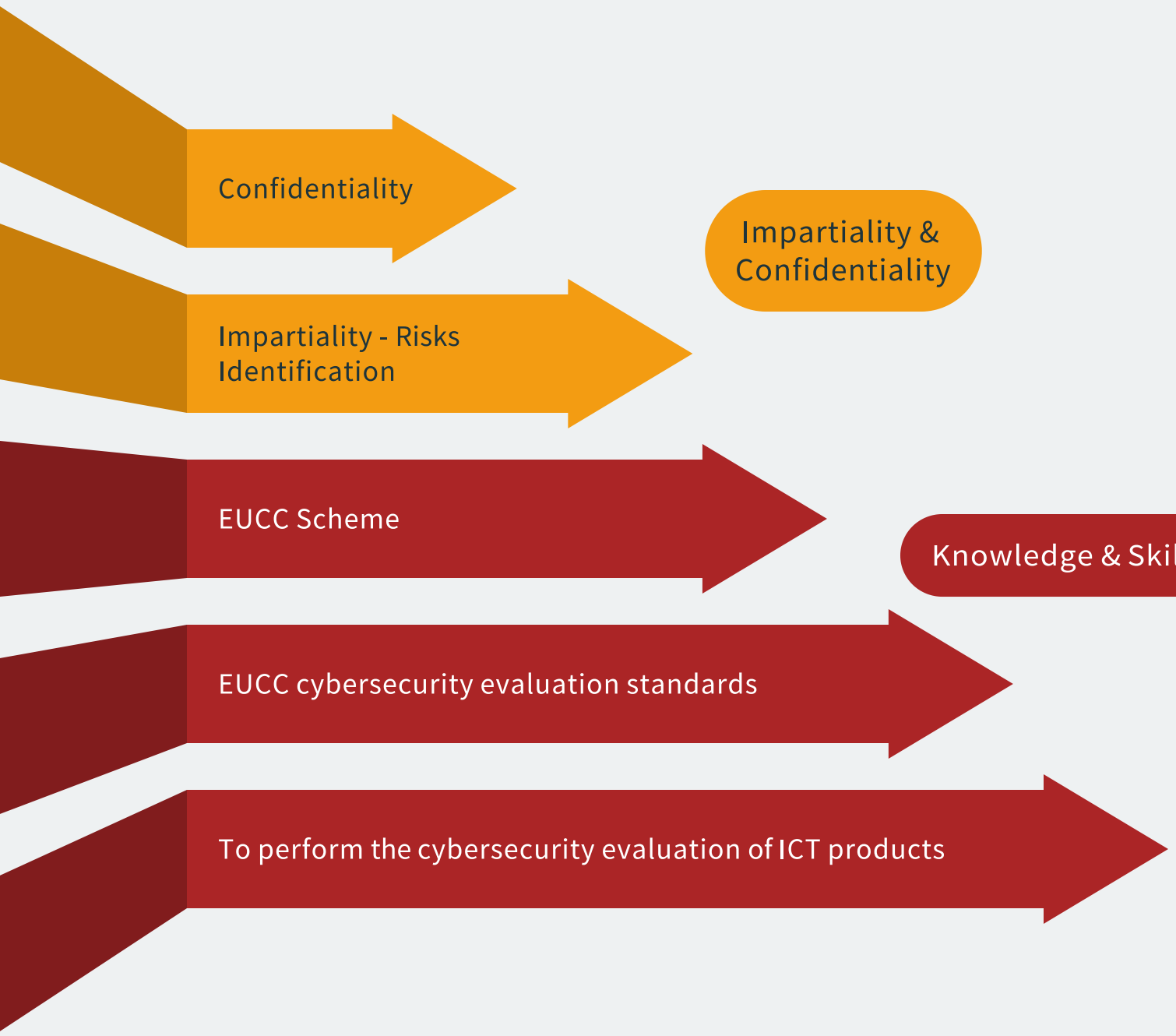
ITSEFs and their evaluators

shall be required to have the **necessary expertise and experience in performing the specific testing activities** to determine the product’s resistance against specific attacks (penetration testing) assuming an attack potential up to ‘Basic’ as described in the CC (AVA_VAN.2 Vulnerability Analysis).

ITSEFs shall define and operate a competence management system for the evaluators taking into account

- knowledge, skills, effectiveness, experience and education (19896-3)
- elements of competence, competency levels and the measurement of the elements of competence (19896-1)
- the types of technology

RED ALERT LABS
IoT Security



Existing Competences

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1

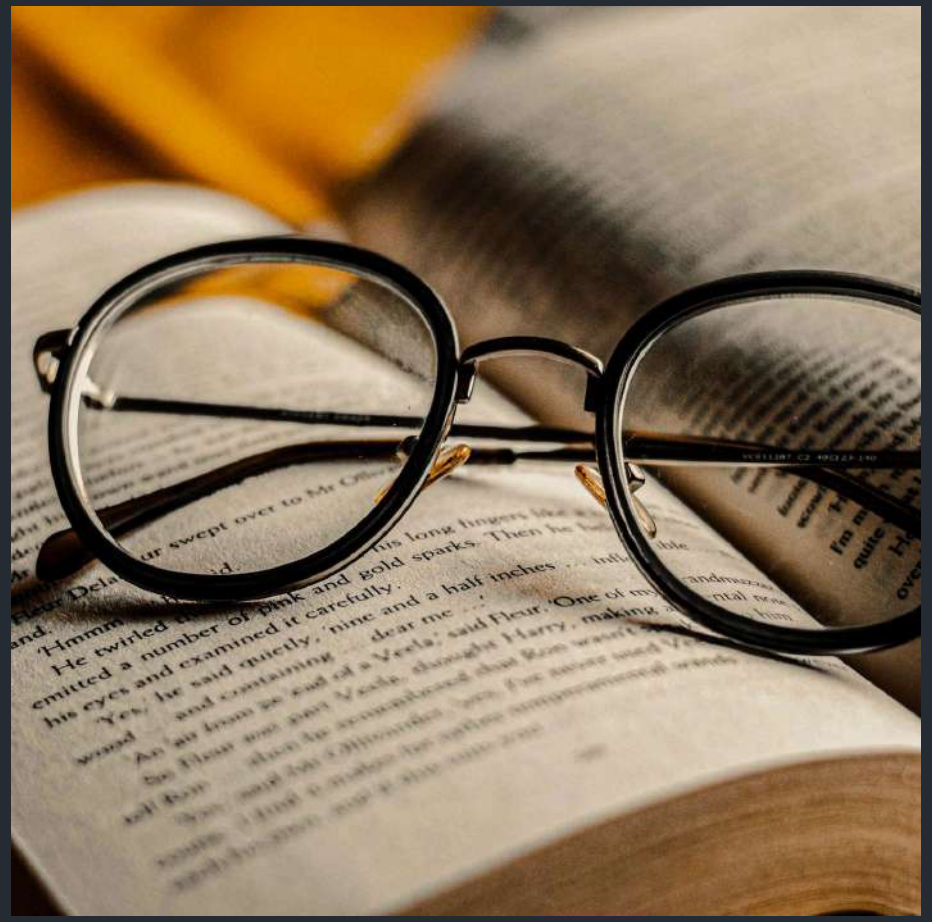
Competencies

- This clause defines the **minimum elements of competence** that should be used by the ISO/ IEC 19896 series when considering the requirements for **competence in conformance-testers and/or evaluators for specific IT product** security assurance standards.
- Competence such as **aptitude, enthusiasm, initiative, leadership, teamwork** and **willingness** can be specified by laboratories or accreditation bodies.

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1



Knowledge (Details in next slides for EUCC)

Relevant to product security assurance standard:

e.g **policies** and **procedures** of relevant approval authorities, accreditation bodies and laboratories; and

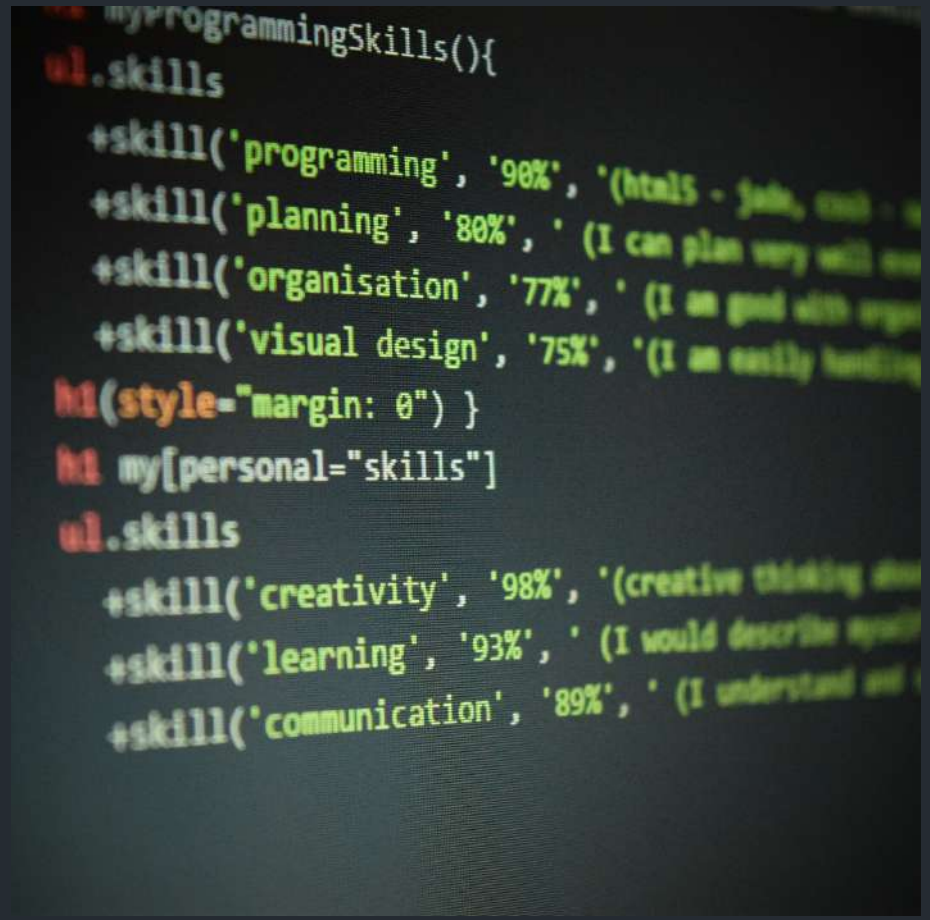
Relevant knowledge classes:

e.g The technology used in the **design, development and deployment** of the products being tested;

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1



Skills

Skills typically required of testers and evaluators of IT security products according to the competency levels defined include:

e.g. being able to **select** or **adapt appropriate evaluation** or **testing method**

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1

Experience

Experienced individuals have:

e.g performed **evaluations** or **conformance-testing**,

e.g perhaps **taught** or **mentored** others over many conformance-testing or evaluation projects

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1

Education

The specification of particular **educational qualifications** such as an **Associate**, **Bachelor's**, or **higher degree** can help to determine an **individual's ability** to follow a formal program or work independently.

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1

Effectiveness

Effectiveness should **consider the accuracy of test results or evaluations obtained**, the ability to **repeat evaluation or test methods** and **activities performed** by other competent testers and evaluators

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1

Competency levels

Level 1 (Associate)

-provide support for some activities

- perform work under supervision

Level 2 (Professional)

-can work unsupervised in some areas

- is able to response to deviations found

Level 3 (Manager)

- work unsupervised in most testing areas

- response to deviations

- able to supervise work of Level 1 and 2

Level 4 (Principal)

- competent in all testing aspects

- communication with stakeholders and approval authorities

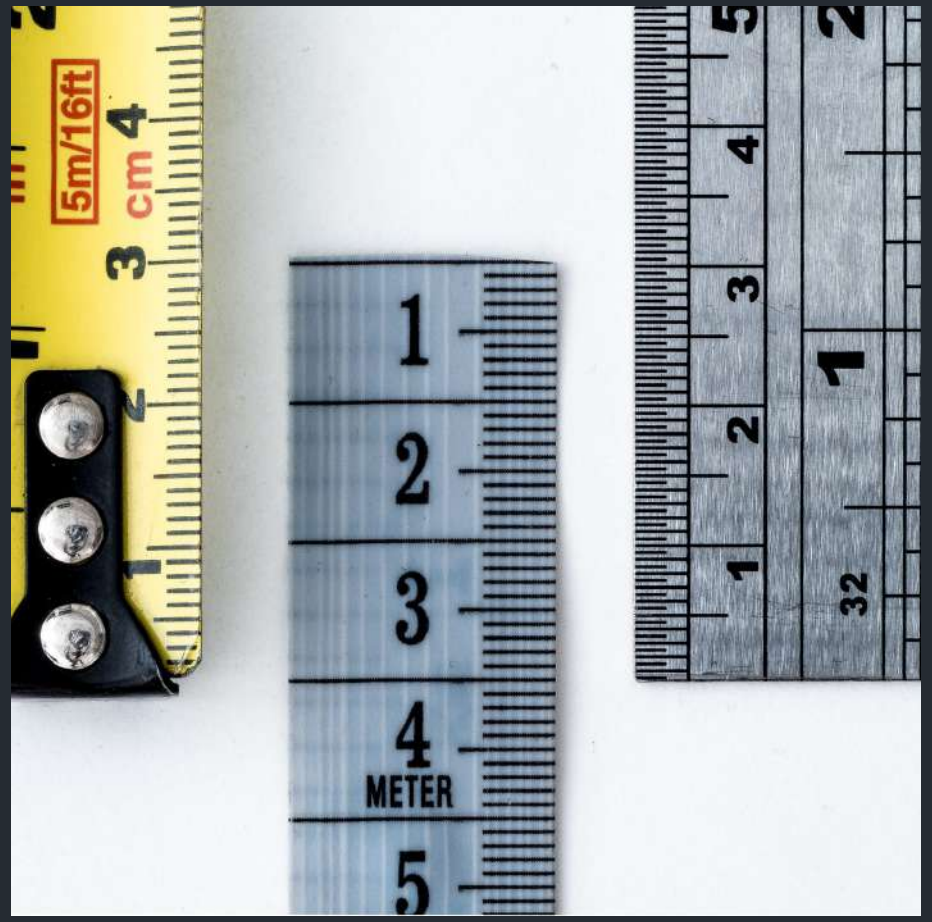
- work unsupervised in all testing areas

- response to deviations deviations and supervise for Level 1, 2 and 3

RED ALERT LABS
IoT Security

Normative Competencies

ISO/IEC 19896-1



Measurement of elements of competences

- Knowledge: e.g. through **professional qualifications**
- Skills: e.g. through **training records**
- Experience: e.g. through **maintaining records** of the **number** of **projects completed**,
- Education: e.g. by the possession of **authentic certificates** issued by **recognized organizations**.
- Effectiveness: e.g. through "**time needed to make a test or evaluation plan**", "**number, type and severity of comments received during internal quality assurance activities**", "**use of direct and focused language in test reports**"

RED ALERT LABS
IoT Security

17025 §6.2 Personnel

Example

This is an extract of our competences reference document which established the evaluators skills scale.

	Level 1 (Associate)
Knowledge Area Name	**Knowledge Area Description**
IT Security Techniques - Competence requirements for Information Security Testers and Evaluators	This area of competence encompasses all the skills necessary to be able to carry out compliance and testing activities in the context of evaluation within the framework of the EUCC (at least substantial level) certification scheme and equivalent.
Skill Name	**Skill Description**
Conformance Testing	Having minimum skills in conformancy testing related to EUCC or other certification schemes (under supervision). Ex: Evaluation ISO/IEC 15408-3 and ISO/IEC 18045
Evaluation Method	Having minimum skills in evaluation methods related to EUCC or other certification schemes (under supervision) Ex: Evaluation ISO/IEC 15408-3 and ISO/IEC 18045
Technical Report Writing	Is able to write some part of observation reports (under supervision).
Security Assurance and security funcational Classes	Having basic knowledges of Security Assurance and security functional requirement classes
Common Technologies	Having basic knowledge when it comes to common technologies
Assurance Paradigm	Having basic knowledges in evaluation authorities, schemes and laboratory management
Experience Required	
Contribution to at least 1 evaluation project and 1 consultancy project related to EUCC or other certification	Contribution to at least one project covering 1 or more technical areas of Red Alert Labs' evaluation technologies scope.
From 0 to 3 years in working undustry	
Education Required	
Tertiary educational qualification, such as an Associate, Bachelor's, or higher degree, that is relevant to the requirements addressed in ISO/IEC 15408 and the evaluation methodology requirements in ISO/IEC 18045.	
Effectiveness Criteria	
Major successful execution of projects: - is capable of executing some tasks of the project properly	**Trainings** Need to follow at least the internal trainings below before being capable to achieve level 2: - CC Essential - ISO 17 025 Essential and ISO 17 025 Processes - Cybersecurity regulations and certifications overview (CSA, EUCC, EUCS, Eurosmart) - Employee Arrival (Cybersecurity and Privacy)
Had knowledge of the existing Laboratoty Management documentation	Is able to give inputs for writing testing plans in some technical areas (undersupervision): - no criteria on time needed to provide these inputs.
Is able to perform some tests under supervision: - no criteria on time needed to execute a test - is capable of repeating tests in 1 or more area - is capable of understanding new technologies	

Normative Competencies

EUCC

Global

1. to have the **necessary expertise** and **experience** in performing the **specific testing activities** to determine the product's **resistance against specific attacks (penetration testing)** assuming **an attack potential of 'basic-enhanced'** as described in the CC (**AVA_VAN.3** Focused Vulnerability Analysis).
2. For the technical domains defined in Chapter 8, SPECIFIC EVALUATION CRITERIA AND METHODS : e.g. **AVA_VAN.4 Methodical vulnerability analysis, AVA_VAN.5** Advanced methodical vulnerability analysis

Normative Competencies

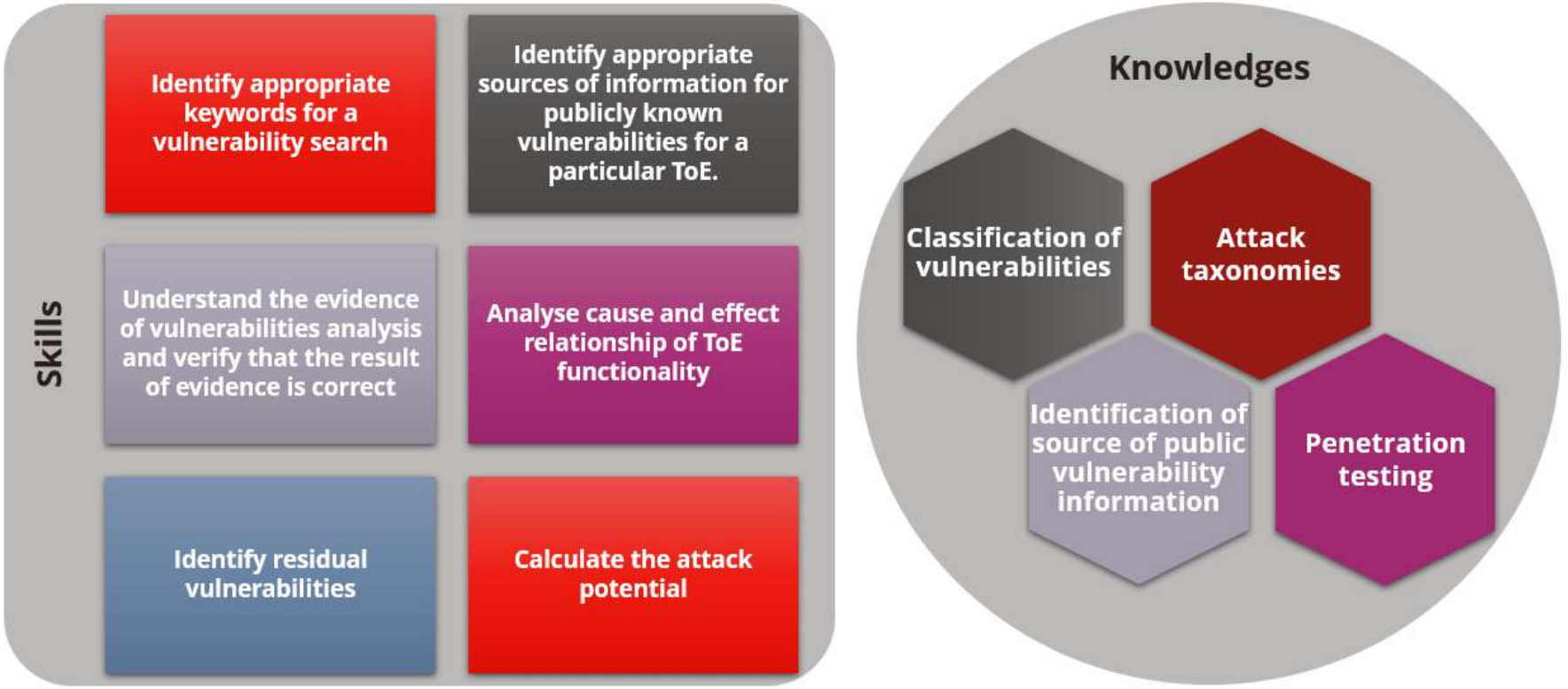
EUCC

Categories Of Minimum ITSEF Requirements For Security Evaluation - Technical Domains

- Smart Cards And Similar Devices: e.g. IC Design and Production Process, Smartcard Integrated Circuit Technology
- Hardware Devices With Security Boxes (HDwSB): e.g. Physical Technology, Physical Specific Attacks

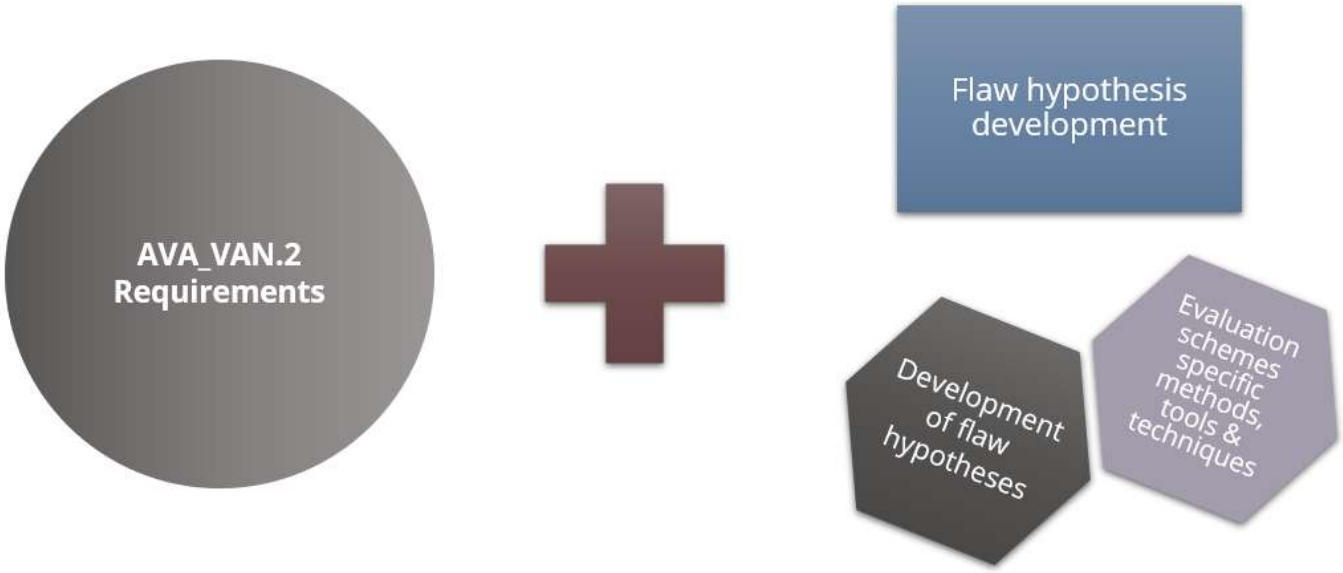
Competences Example

ISO/IEC 19896-3 - competencies and knowledge for evaluators for **substantial** level (**AVA_VAN.2**)



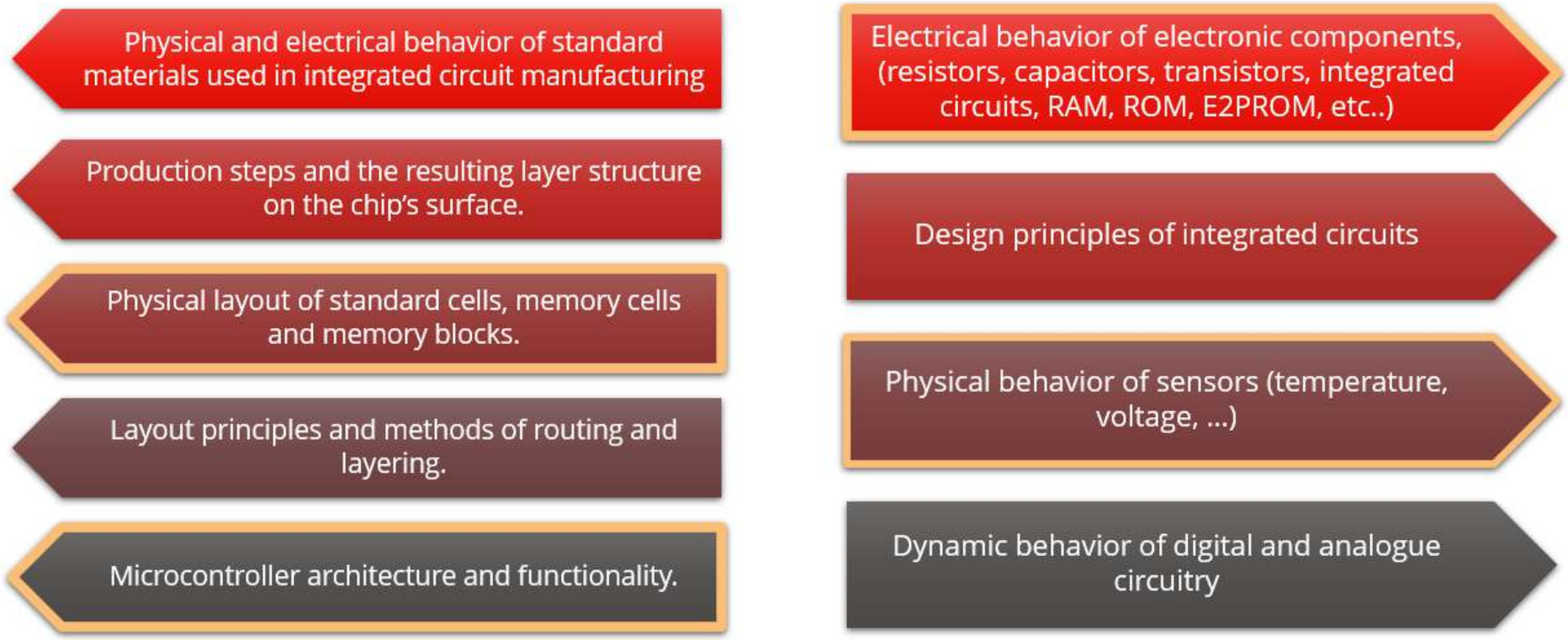
Competences Example

ISO/IEC 19896-3 - competencies and knowledge for evaluators for **high** level (AVA_VAN.5)



Competences Example

EUCC - Example of Specific skills and knowledge for IoT's test



Facilities Example

Reminder ISO 17025

- **Environmental conditions must not adversely affect result validity.**
- **Labs must document the facilities and conditions needed for correct performance of the lab.**
- **Labs must monitor, control & record environmental conditions that affect validity of results.**
- Measures to control facilities must be implemented and monitored
- Labs must ensure conditions are met in cases where lab activities are performed in facilities outside its control.

Facilities Example

Additional requirement to ISO/IEC TS 23532-1:2021, 6.3.1.1

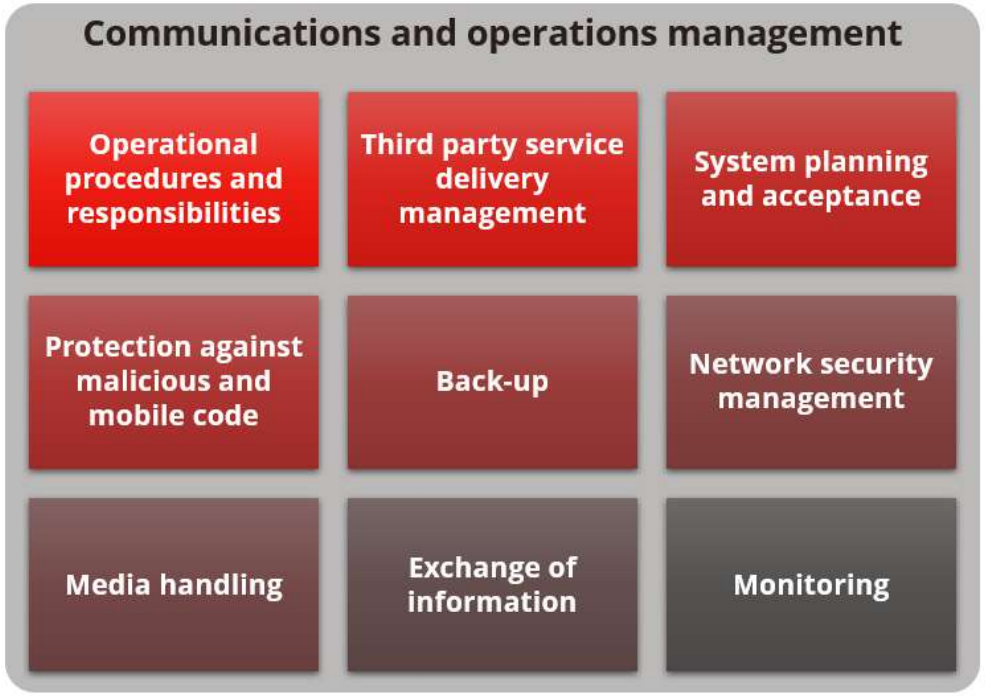
Network isolation

Network isolation must ensure both the accuracy and integrity of the test results and their confidentiality.

RED ALERT LABS
IoT Security

Facilities Example

EUCC - Example of site security requirements



Other specific actions required

This page gives example of how we can address various requirement of the ISO 17025 and other standards.

Access control

- Enterprise access control
- Lab access control
- Privacy window film

Sensitive area monitoring

- Camera
- Physical Access log

Network isolation

- Enterprise network
- Isolated lab network

Additional system

- Share folder and archiving system (1 for enterprise & 1 for lab)
- Issue tracking system
- Backup system

RED ALERT LABS
IoT Security

Equipment Example

Reminder ISO 17025

Labs must have access to equipment necessary for the correct performance of lab activities.

Labs using equipment outside their control must ensure that the equipment meet the requirement of this document.

Labs must have a procedure for handling and maintenance of equipment.

Labs must ensure that equipment conform to specifications before being put into or returned to service.

Equipment must be able to provide a valid result.

Equipment must be calibrated according to a defined calibration program

Devices with expiry date for calibration must be labeled

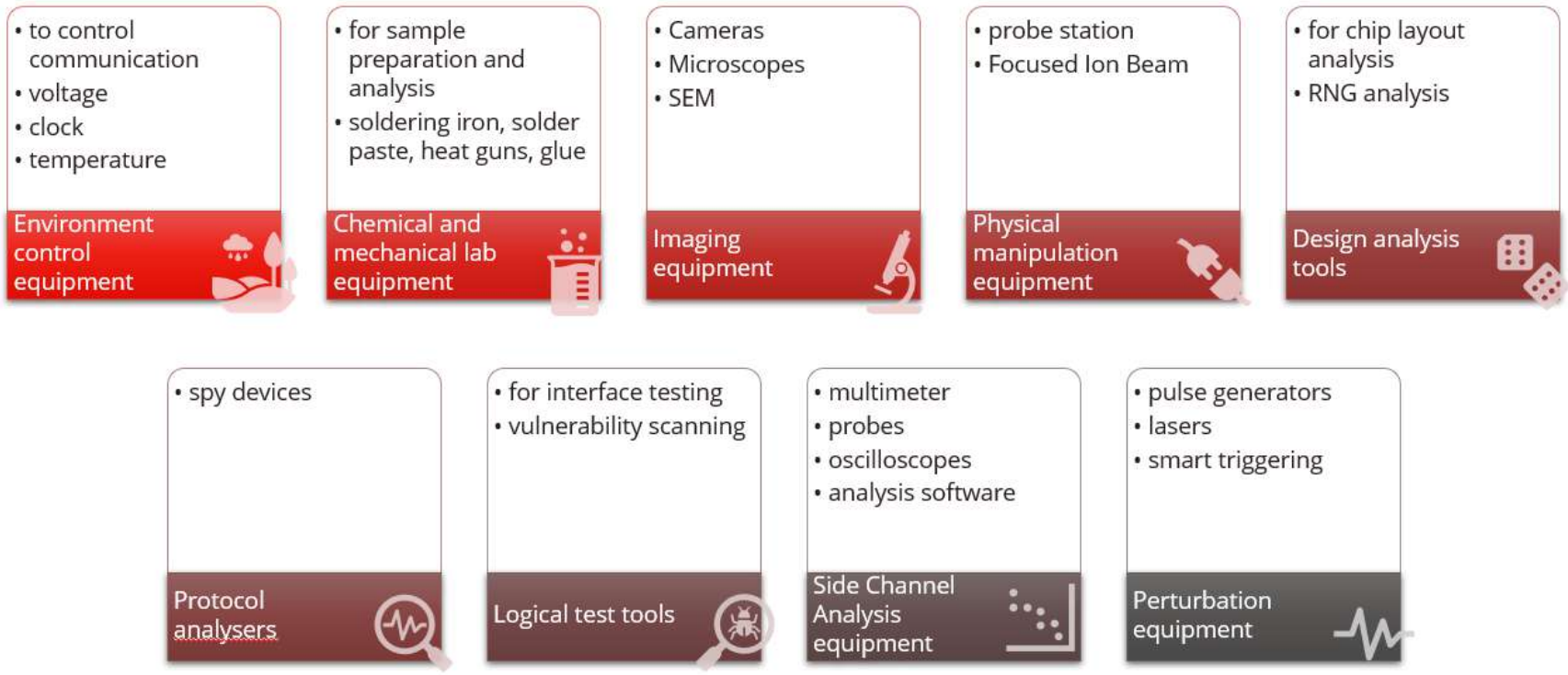
Unintended changes to equipment must be prevented

Maintain records about equipment , their location, calibration date, reference materials, equipment repairs, etc

RED ALERT LABS
IoT Security

Equipment Example

EUCC - Example of required equipment



Standards & Documentations Compliance

EUCC ITSEF

Standards to take into account

To build Lab system management

- **ISO/IEC 17025:2017**
- **ISO/IEC 19896-1:2018**
- **ISO/IEC 19896-3:2018**
- **ISO/IEC TS 23532-1:2021**
- ISO/IEC TS 19608
- ISO/IEC 17000

To perform EUCC activities

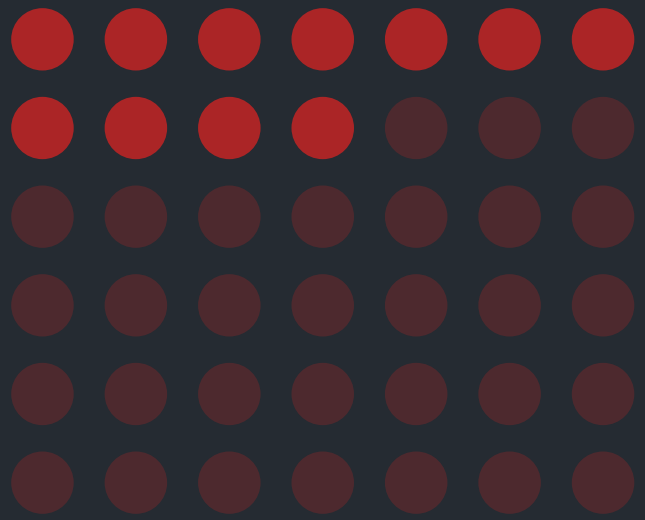
- ISO/IEC TR 15446
- **ISO/IEC 15408-1**
- **ISO/IEC 15408-2**
- **ISO/IEC 15408-3**
- **ISO/IEC 18045**
- ISO/IEC 20543:2019
- ISO/IEC 18367

RED ALERT LABS
IoT Security

Documentation to be compliant to ISO 17025 + EUCC

~80 documents in our Laboratory management system

25%

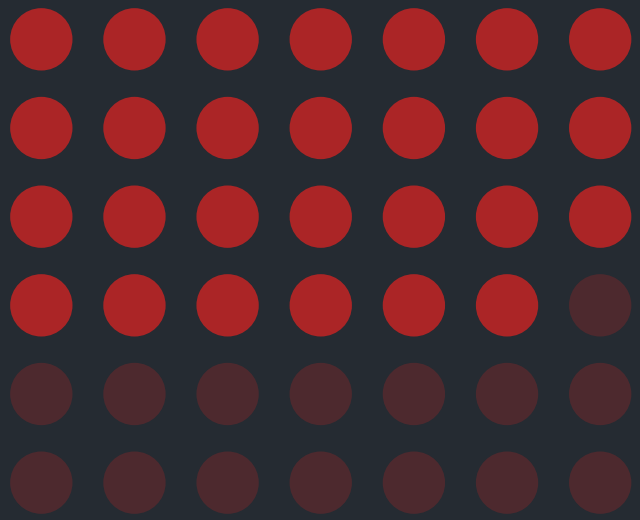


Procedures

Describes rules and process.

Each activities which fall in the scope of the accreditation is documented through these documents.

63%



Forms

Related to procedures, documents to fulfilled during quality process, proof that the process and rules are applied.

12%

Others (Template, WI, ...)

Others documents which can help users of the management system

RED ALERT LABS
IoT Security

Example of how do we take into account the EUCC in our Lab management system?

ID	Name	ISO 17025
P-500	Management responsibility	§4.x + §5
P-610	Resource-Management	§6 + §6.1 + §6.3
P-620	Competence-Awareness-and-Training	§6.2
P-645	Control-Monitor-Measure-Equipment	§6.4 + §6.5
P-660	Control-External-Providers	§6.6
P-710	Customer-Related-Processes	§7.1
P-720	Operational-Planning-of-Methods	§7.2 + §7.3
P-740	Handling-test-cal-items	§7.4
P-755	LMS-Monitor-Analysis-Evaluation	§7.5 + §7.6 + §7.7
P-780	Reporting of Results	§7.8
P-790	Complaints-Nonconforming-Outputs	§7.9
P-820	Control of documented information	§8.2 + §8.3 + §8.4
P-850	LMS-Risk Management-Planning	§8.5
P-860	Improvement	§8.6
P-870	Nonconformity-Corrective-Action	§8.7
P-880	Internal-Audits	§8.8
P-890	Management-Review	§8.9

- Addition of special EUCC requirements in procedures

  We amended the content of each procedures to take into account the new requirements highlighted by the AHWG.

- Special EUCC procedures & new processes consideration

  This document relates to EUCC, in particular with the clauses dealing with Composite evaluation, Monitoring compliance, assurance continuity and patch management.

  This document also take into account the “EUCC accreditation requirements for RED ALERT LABS activities at substantial assurance level.” Provided by ENISA

- Pilot Evaluation

RED ALERT LABS
IoT Security

17025 §6.2 Personnel

Example

This is an example of our procedure which frames everything related to personnel.

3 rue Parmentier
94140 Alfortville
France
Tel. +33 (0)6 48 37 95 88
www.redalertlabs.com

Red Alert Labs (S.A.S.U)
Société par actions
simplifiée à associé unique
Au capital de 10 000,00 €
827 677 303 R.C.S. Créteil

5.3.2. The LMS team leader is on alert for opportunities to improve organizational knowledge. An information library is maintained to collect and make available information that can enhance knowledge.

5.3.3. Red Alert Labs laboratory manager notifies by default both the relevant approval authority and accreditation body within 30 days of any change in key personnel. When key laboratory staff are added, the notification of changes includes a current resume for each new staff member.

5.3.4. Red Alert Labs maintain a list of personnel (Record "RC-620 Roles and responsibilities") designated to fulfill laboratory requirements including:

5.3.4.1. Laboratory director/Laboratory Manager,

5.3.4.2. Approved Report signatories,

5.3.4.3. Evaluation team leaders, and

5.3.4.4. Evaluators.

5.4. Each manager is responsible for identifying job specific training requirements for each position in their area and to maintain the employee training summaries in the "RC-620-Matrix-Skills" record. Recommended training are also maintained in the record "RC-620-Recommended trainings summary" by the Laboratory Manager.

5.4.1. Actions to acquire the necessary competence can include mentoring, provision of training, the reassignment of current employees, or the hiring or contracting of competent personnel.

5.5. When an employee is hired, changes positions or job requirements change, Human Resources obtains a resume or application from the employee to document their qualifications.

5.5.1. Employee qualifications are compared against the requirements for the position. If there are requirements that the employee's qualifications do not meet, human resources manager or the employee's manager identifies an action plan to provide the employee with the necessary qualifications.

EUCC Procedure

Example

This is an example of our main EUCC procedure which frames everything related to additional EUCC requirements.

3 rue Parmentier
94140 Alfortville
France
Tel. +33 (0)6 48 37 95 88
www.redalertlabs.com

Red Alert Labs (S.A.S.U)
Société par actions
simplifiée à associé unique
Au capital de 10 000,00 €
827 677 303 R.C.S. Créteil

1

1. Purpose/Scope

1.1. The purpose for this procedure is to establish the process related to EUCC specificities

1.2. The procedure applies to the laboratory activities related to EUCC evaluation.

2. Responsibilities and Authorities

2.1. The Laboratory Manager has the prime responsibility and approval authority for this procedure.

2.2. In support of the Laboratory manager, the LMS team is responsible for identifying the appropriate recording, evaluation, and monitoring.

3. References and Definitions

3.1. This document relates to EUCC, in particular with the clauses dealing with Composite evaluation, Monitoring compliance and patch management.

3.1.1. This document also take into account the "EUCC accreditation requirements for RED ALERT LABS activities at substantial assurance level." provided by the ENISA

3.2. References

3.2.1. Cybersecurity Certification, EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, v1.1.1 | May 2021.

3.3. Definitions

3.3.1. Non-compliance: not-fulfilment of a requirement related to provisions of the scheme or certificate.

3.3.2. Non-conformity: not-fulfilment of a requirement related to technical standards or security objectives defined in Article 51 of the CSA.

3.3.3. CB: Certification body

#7 GET INVOLVED

ENISA, SCCG, ISAC, Events, Standards, ICCC, ...

RED ALERT LABS
IoT Security

ENISA Activities

ENISA workshops, webinars around cybersecurity certification

Industrial Organisations

Eurosmart, GlobalPlatform, local ones...

ISACs/MO

Scheme Maintenance Organisation (MO) as an Information Sharing and Analysis Centers (ISACs) covering attack methods, evaluation methdologies, PPs, Crypto, etc.

Events

1. ICCC (Common Criteria Conference)
2. CyberAct Conference
3. ENISA conferences
4. Cybersecurity events

Standards

CEN-CENELEC JTC13 WG3 activities

ISO/IEC JTC1/SC27 WG3 activities

ETSI TC Cyber activities

...

Stay up to date and Contribute...

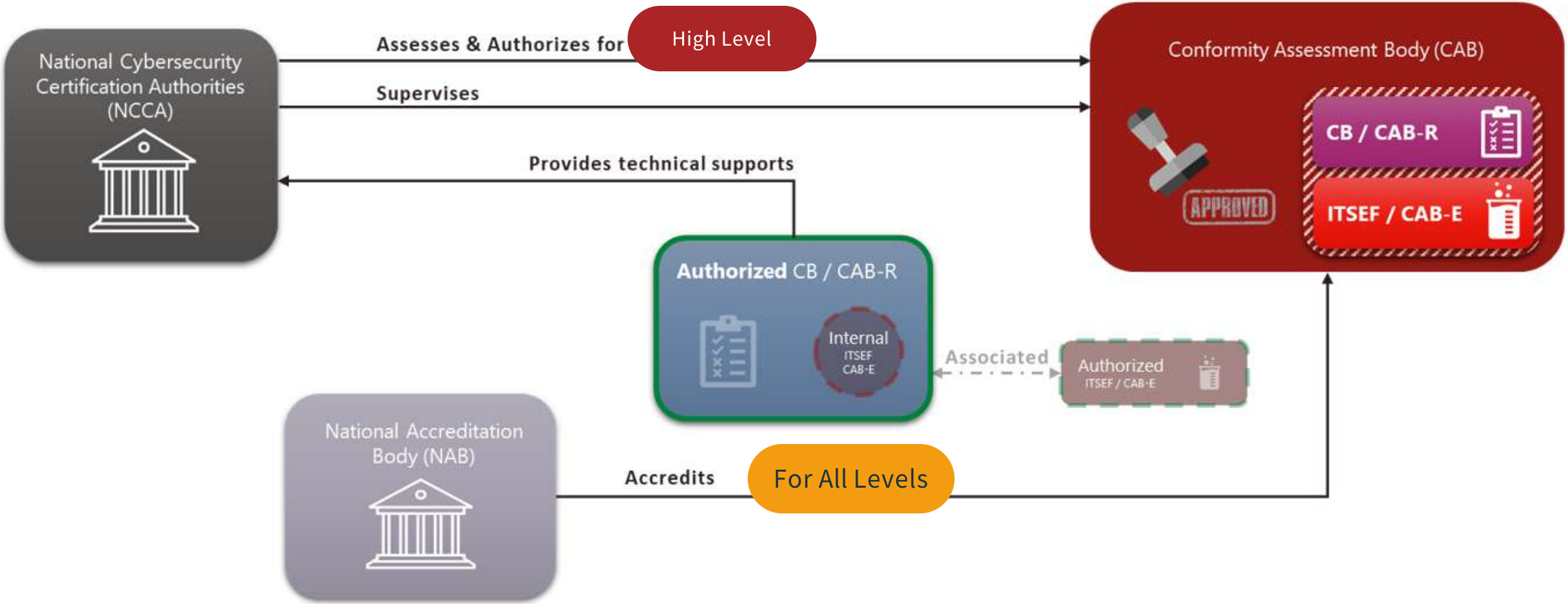
RED ALERT LABS
IoT Security

#8 ACCREDITATION

start official accreditation process

RED ALERT LABS
IoT Security

Accreditation & Authorization



Accreditation

French process example

For Assurance Level SUBSTANTIAL & HIGH

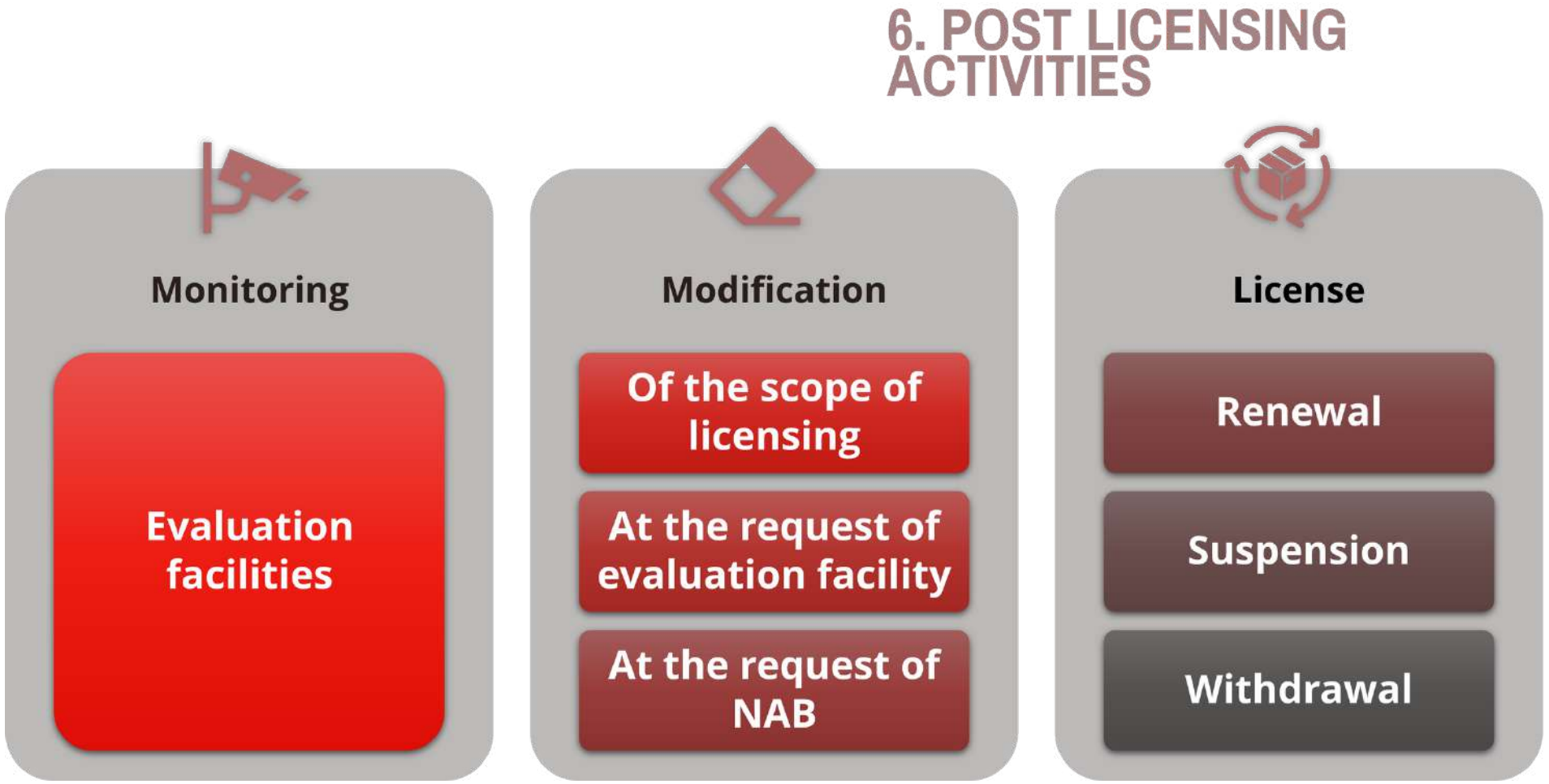
Authorisation

French process example

For Assurance Level High

Authorisation

French process example



#9 RUN PILOT PROJECTS

at least 2 pilot projects

RED ALERT LABS
IoT Security

The objectives of the EUCC pilot Project

Put in practice all the learning and activate processes

- Activating ISO 17025 processes for EUCC

Get hands-on tools and equipments

- Exploring Technical Competences

Identify potential gaps

Authorisation & Peer Assessment

RED ALERT LABS
IoT Security

Key elements

TOE

Applied Certification Scheme

European Cybersecurity Certification Scheme - EUCC

Conformance Claimed

Common Criteria version 3.1 revision 5 (or v4)

Assurance Level

Substantial / High

RED ALERT LABS
IoT Security

Vendor Key Benefits

Trust & Transparency

Create assurance for their consumers while leveraging transparency and trust in your products

Marketing Differentiation

Security is not a feature! They can show the Value of their Secure Solution

Access New Markets

Keeping up with new regulations nationally and internationally

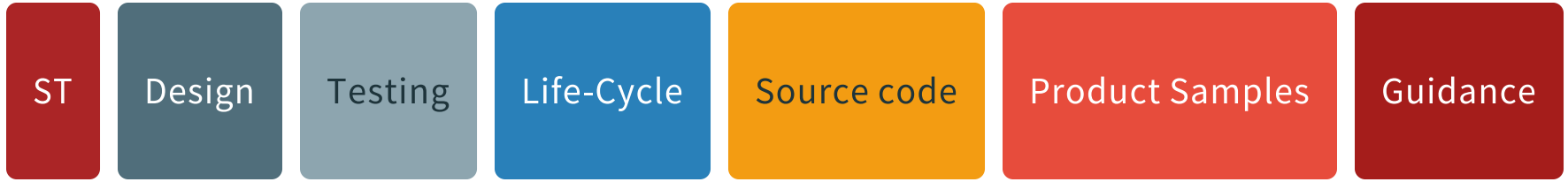
Costs Decrease

By securing their products, they minimize the risks for cyber breaches to occur, and therefore reduce the costs related to it

RED ALERT LABS
IoT Security

Provide Evidence

To Send to the ITSEF



RED ALERT LABS
IoT Security

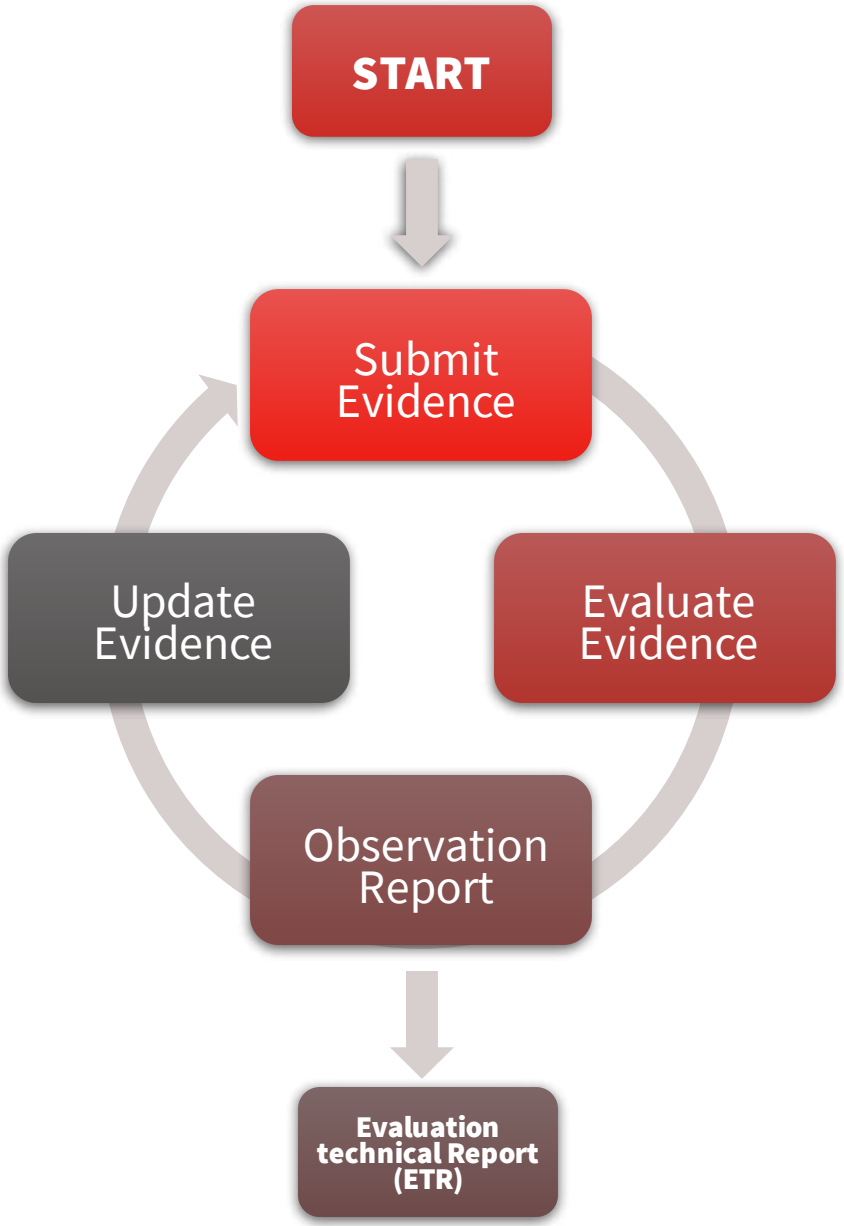
EVALUATION PROCESS
CC Evaluation Methodology

- If the evaluator find an inconsistency or some missing information or error in the evidence documentation

==> produces an OR

Up to you to decide on giving much information on how to rectify the situation or not.

Never provide ambiguous feedback such as FSP are inconsistent with ST



Evaluation Approach

1 | Thorough reading of the elements using information from technical control sheets;

2 | Pooling of technical control sheets during an informal review;

3 | Where appropriate, conduct independent traceability analysis;

4 | Comparison with Common Criteria evaluation requirements;

5 | Establishing verdicts;

6 | Drawing up of the current Technical Evaluation Report for the corresponding component

7 | Verification of report by the ITSEF technical manager.

RED ALERT LABS
IoT Security

CEM

RED ALERT LABS
IoT Security

CEM

Common Methodology for Information Technology Security Evaluation

Sample of Evaluation activities in scope for a TOE

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

2.3 Conformity to an insurance packet

The level of evaluation assurance aimed for by this security target is EAL2+ (or augmented EAL2), augmented by the following components :

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1
- AVA_VAN.3.

Reports produced by the ITSEF

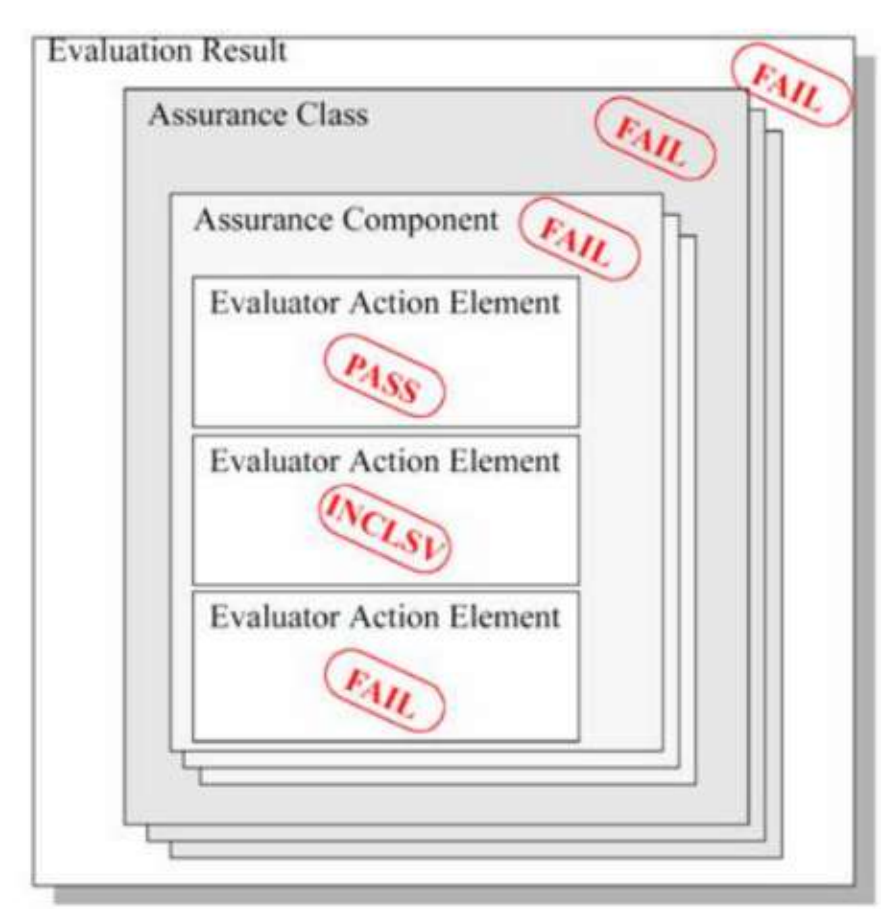
Evaluation Technical Report (RTE)

Focus on your top three content marketing campaign objectives.

CC evaluation labs are required to produce and send reports to the national scheme

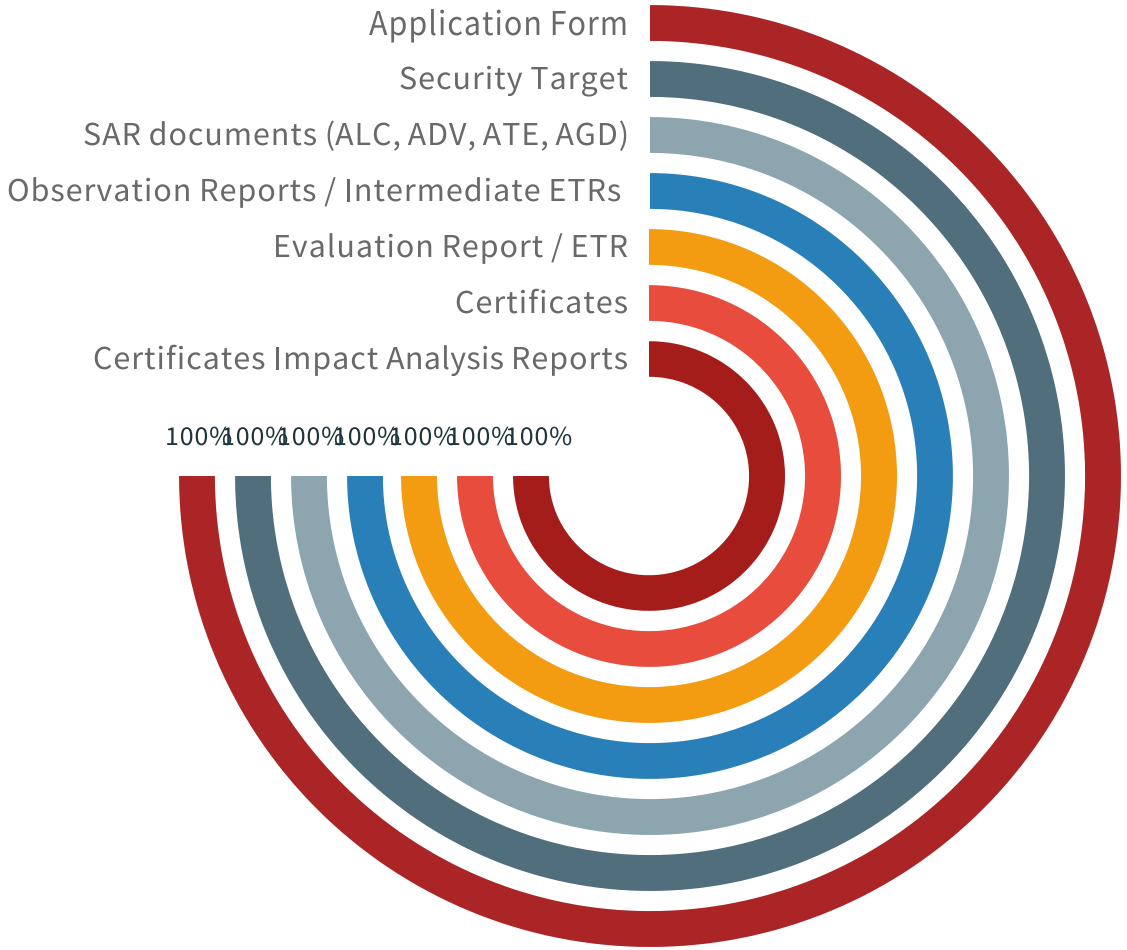
These report summarize the evaluation progress including the status and disposition of issues and comments reported to the vendor

A final ETR is submitted to the Scheme when all the evaluation activity work units have been completed



RED ALERT LABS
IoT Security

Pilots Achievments (EUCC)



RED ALERT LABS
IoT Security

RE-CERTIFICATION/ASSURANCE CONTINUITY

ASSUMPTION

CC certificates are only valid for a single version of a product.

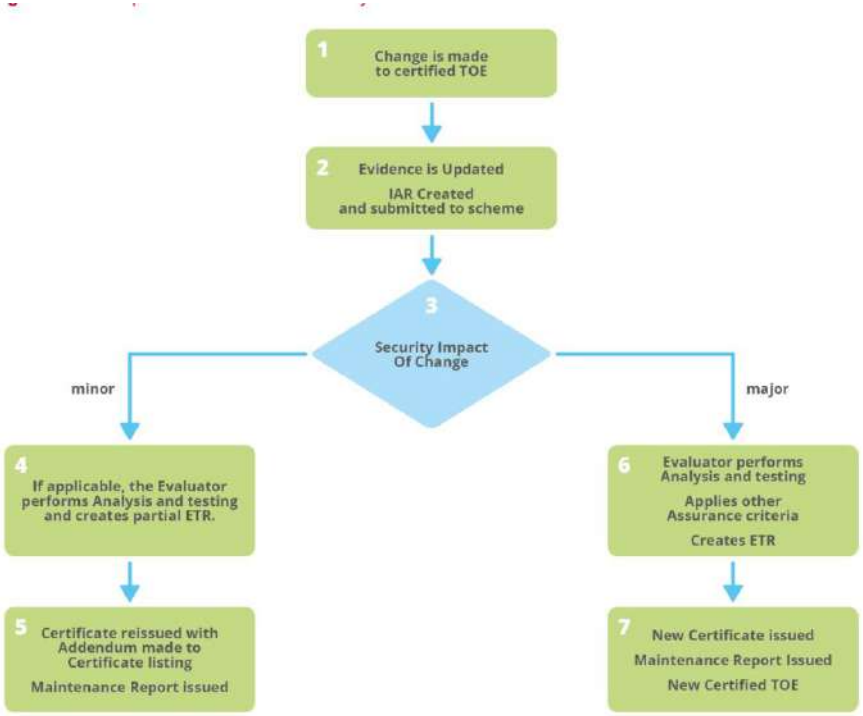
GOAL

Shorten the re-evaluation cycle for previously evaluated product

HOW TO DO ?

Provide evidence that changes in the newer version of the product do not compromise the security claims and evidence presented in the prior version's evaluation.

An Impact Analysis Report (IAR) is submitted to the same evaluation lab that performed the original evaluation.



Content to be updated when slides are finalized @Roland

PARTIAL ETR
RE-ASSESSMENT
RE-EVALUATION
DEVELOPMENT ENVIRONMENT
RE-ASSESSED TOE

IMPACT ANALYSIS REPORT

ASSURANCE CONTINUITY

SUBSET EVALUATION
MAINTAINED CERTIFICATE
CERTIFIED TOE
CHANGED TOE
DEVELOPER EVIDENCE
ASSURANCE BASELINE
SECURITY TARGET
MAINTAINED TOE
IAR
CERTIFICATE ADDENDUM

RED ALERT LABS
IoT Security

IAR table of content

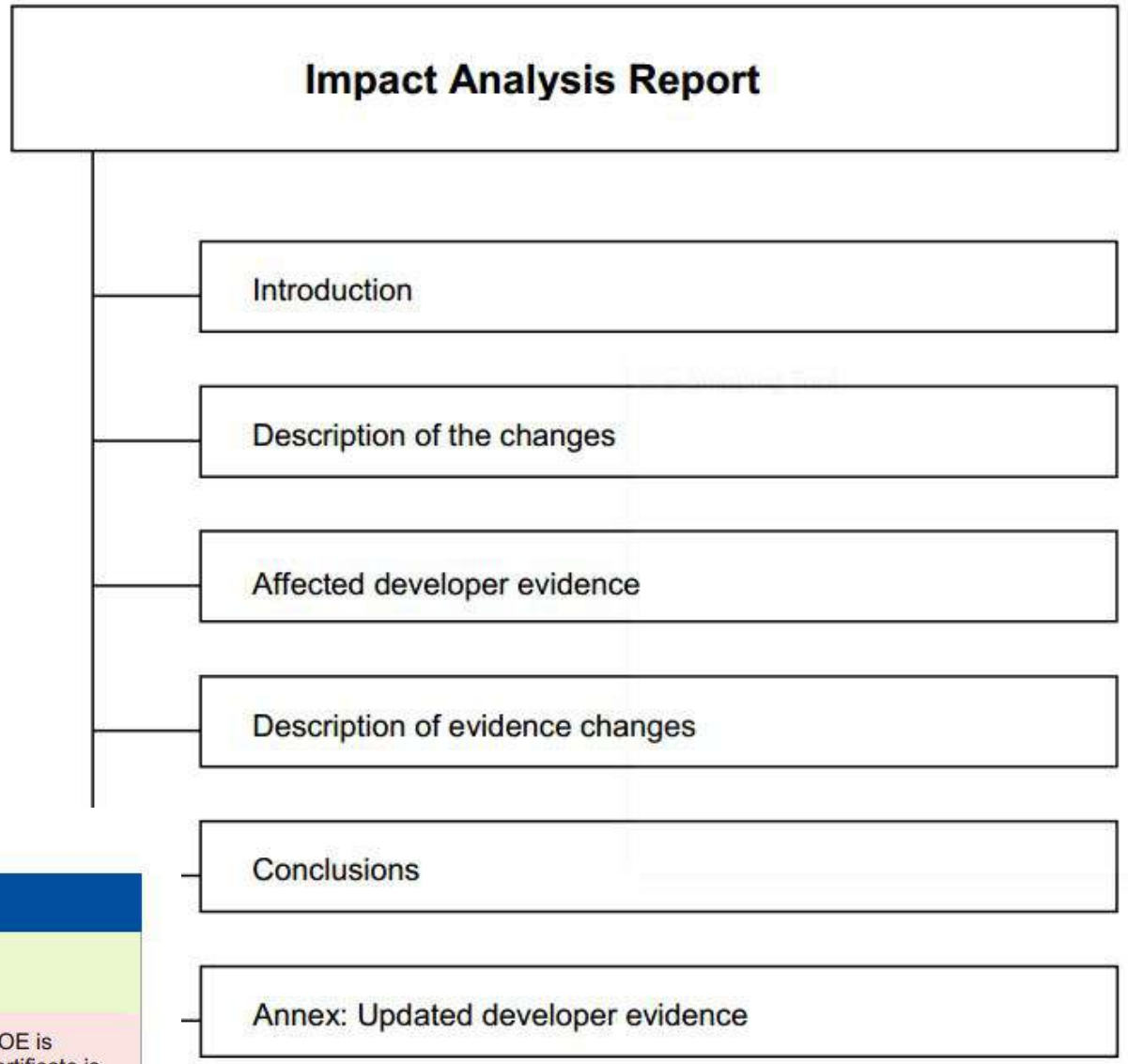


Table 1: Impact of re-assessement results on certificates

Re-assessment results	Impact on the certificate
Positive[66]	The validity of the initial certificate is extended into the renewed certificate.
Negative	The new AVA_VAN level reached by the re-assessed TOE is indicated into a re-issued certificate, and the previous certificate is archived.

#10 SHARE, UPGRADE & MAINTAIN

Test and Learn, increase capacities

RED ALERT LABS
IoT Security

ENISA Activities

ENISA workshops, webinars around cybersecurity certification

Industrial Organisations

Eurosmart, GlobalPlatform, local ones...

ISACs/MO

Scheme Maintenance Organisation (MO) as an Information Sharing and Analysis Centers (ISACs) covering attack methods, evaluation methdologies, PPs, Crypto, etc.

SHARE

Events

1. ICCC (Common Criteria Conference)
2. CyberAct Conference
3. ENISA conferences
4. Cybersecurity events

Standards

CEN-CENELEC JTC13 WG3 activities

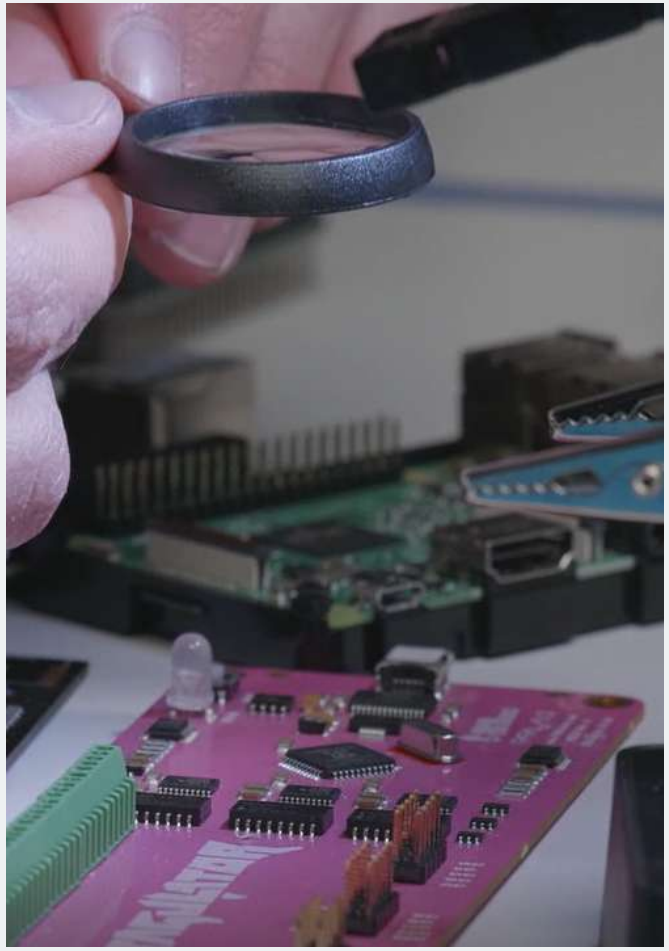
ISO/IEC JTC1/SC27 WG3 activities

ETSI TC Cyber activities

...

RED ALERT LABS
IoT Security

Upgrade Gradually your Team & Laboratory



Security Assurance Levels

- from Basic
- to Substantial
- to High

Scope

- ICT/IoT Products, Processes and Services
- HW & SW
- Cloud Services
- Network Infrastructure
- Mobile Applications

Conformity & Vulnerability Assessment Approaches

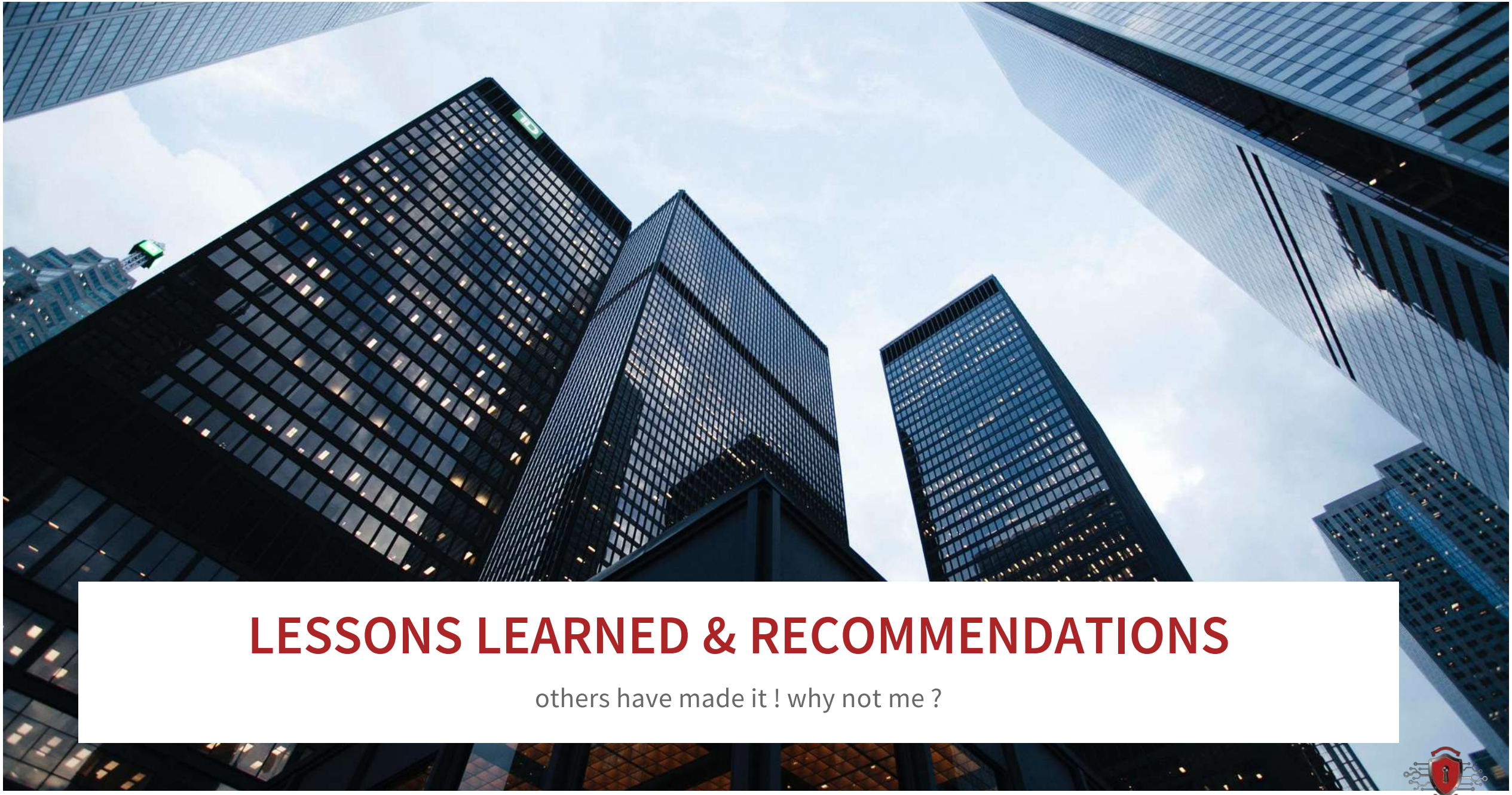
- Black Box
- Gray Box
- White Box

Expertise

- Get Recognized Consultants and Evaluators
- Get more experience in the field
- Get other accredited

ISO/IEC:17025 standards.

RED ALERT LABS
IoT Security



LESSONS LEARNED & RECOMMENDATIONS

others have made it ! why not me ?

RED ALERT LABS
IoT Security

BEST PRACTICES & LESSONS LEARNED
YOUR ROADMAP TO SUCCESS AS AN ITSEF

THANK YOU

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

DISCUSSION

CLOSING REMARKS

- Proposal for Cyber resilience act
- Why and how to become a CAB for the EUCC scheme
- How a Certification Body operates
- How to build and operate a testing laboratory in the context of EUCC
- Next steps by NÚKIB

Národní úřad
pro kybernetickou
a informační bezpečnost

THANK YOU VERY MUCH !

Ing. Markéta Šilhavá
m.silhava@nukib.cz
+420 702 160 590

Bc. František Grossmann
f.grossmann@nukib.cz
+420 720 061 890

ncca@nukib.cz