RED ALERT LABS
IoT Security

TrustBoost Training - Day 1

CyberSecurity Act (CSA) & Cyber Resilience Act(CRA)

Co-funded by the European Union

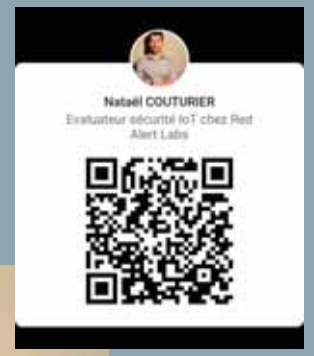
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

TrustBoost

17/10/2024

Who's who around here?!

Sreedevi Beena, Senior Cybersecurity Analyst & Evaluator



Nataël Couturier, IoT Security Evaluator & Quality Manager

RED ALERT LABS
IoT Security

Our Services

SECURITY CONSULTING

- Gouvernance Cyber
- Security By Design
- Security Hardware/Software
- IoT Framework Assurance

SECURITY EVALUATION

- Pentesting
- Regulations
- Standards
- Certification

SECURITY INNOVATION

- Scan Vulnerability
- Risk analysis
- Automatisation Process

SECURITY TRAINING

- Cybersecurity Act
- Certification Scheme
- Common Criteria
- IoT Cybersecurity

RED ALERT LABS
IoT Security

Our references

Clients, Partner & Affiliations

RED ALERT LABS
IoT Security

Red Alert Labs History

Agenda

1. CSA
   1. Context
   2. Introduction
   3. Certification Activities
   4. Impact of the CSA on NCCA's missions
2. CRA
   1. Context
   2. Scope
   3. Main Requirements
   4. CSA vs CRA

RED ALERT LABS
IoT Security

Challenges

125 Bn+
of IoT Devices

2030

50%+ are vulnerable

62% of attacks exploit customers' trust in their suppliers.

> "Supply Chain attacks such as Solarwinds worry me, because I don't see at this point how we can protect ourselves from it. Even for a company that strictly follows all the recommendations of the ANSSI - and that doesn't exist - it will remain very complicated."

Guillaume Poupard,
ANSSI ex-CEO, 2022

> "The lack of transparency and the inability to conduct audits (expertise, time, costs) lead to a serious a serious risk for trust within the supply chain."

Supply Chain
report, ENISA 2021

RED ALERT LABS
IoT Security

Trust

Technical Means

evaluation methods, security architecture review, code auditing and testing, of course

Social Means

reputation and transparency of stakeholders

Legal Means

contracts (commitment or liability) and regulations

RED ALERT LABS
IoT Security

Certification / Conformity Assessment

“Cybersecurity **certification** is the attestation of a product's robustness carried out by a third-party assessor, according to a scheme and reference framework adapted to users' security needs and taking account of technological developments.” **ANSSI**

Laboratory

Certification Authority

Accreditation Authority

CAB

NAB

Conformity Assessment is the process of testing, inspection and certification determining if a product, service, system, or body meets specified requirements

RED ALERT LABS
IoT Security

EU Laws and Regulations related to ICT/IoT Products Cybersecurity

EU Cybersecurity Act (CSA)

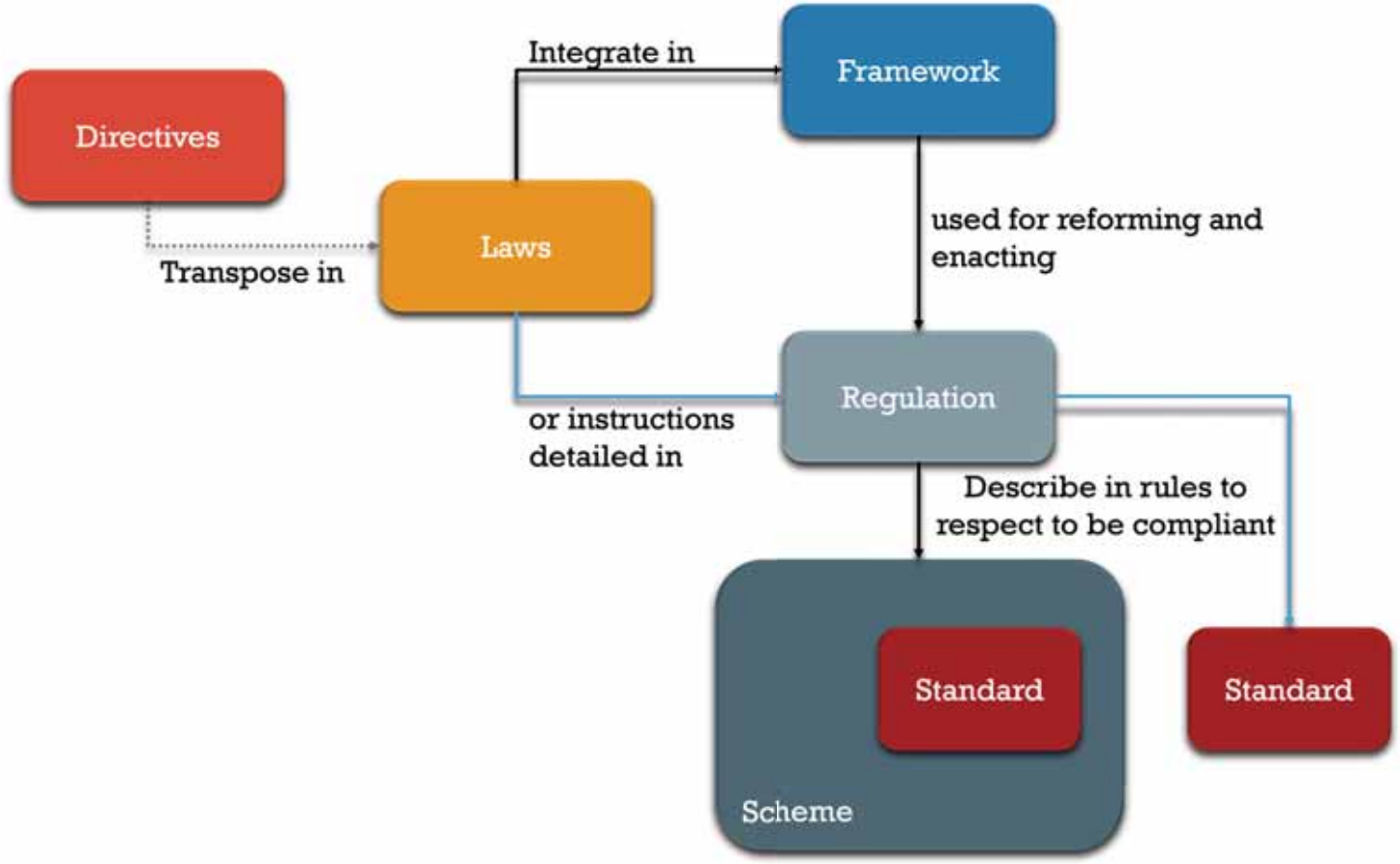
Cyber Resilience Act (CRA)

Radio Equipment Directive (RED) - DA

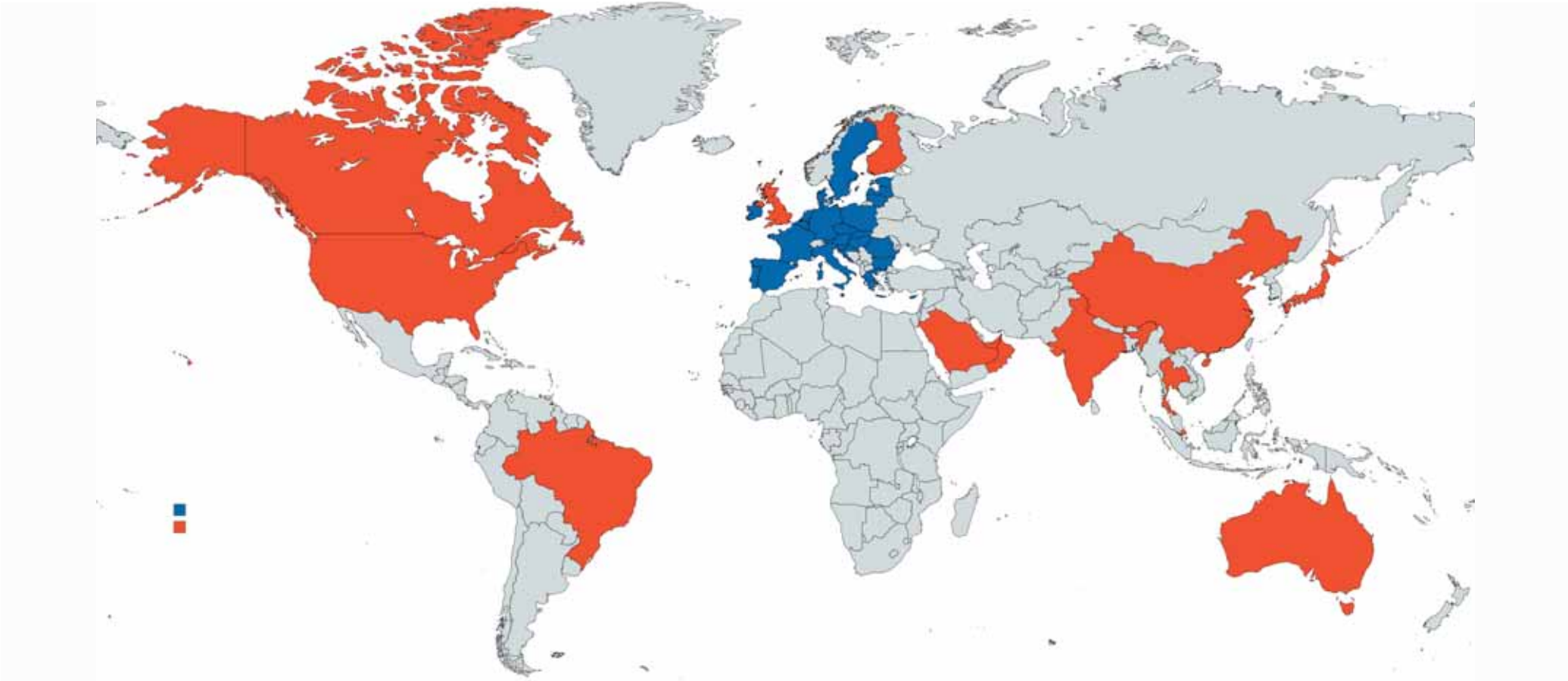
GDPR; NIS2, ...

It is essential for Manufacturer addressing the EU market to comply with these laws and regulations in order to avoid significant fines and reputational damage. Monitoring and adapting products accordingly is key to staying compliant.

From Directives to Standards



IoT Cybersecurity Standards & Regulations - RAL coverage



Regulation and Standards with Impact on Europe

RED ALERT LABS
IoT Security

Cybersecurity Act (CSA)

CSA - Subsection 1

Overview

What is CSA?

Regulation (EU) 2019/881 of the European Parliament.

European **CyberSecurity Act** strengthens the EU Agency for cybersecurity (**ENISA**) and establishes a cybersecurity certification framework for products and services.

RED ALERT LABS
IoT Security

REGULATION (EU) 2019/881

Cybersecurity act

TRUST

"trust should be further strengthened by offering information in a transparent manner on the level of security of ICT products, ICT services and ICT processes ..."
"An increase in trust can be facilitated by Union-wide certification providing for common cybersecurity requirements and evaluation criteria across national markets and sectors."

ADOPTION

The Council of the European Union adopts the Cybersecurity Act on June 7, 2019.

ASSURANCE LEVELS

Cybersecurity Act define 3 assurance levels.

- Basic
- Substantial
- High

FRAMEWORK AND STRUCTURE

.

European CyberSecurity Act Objectives

- Strengthens ENISA (the EU Agency for cybersecurity)
  Granting a permanent mandate, more resources andadditional tasks
- Establishes a cybersecurity certification framework
  Allowing European cybersecurity certificates to berecognised across the European Union

RED ALERT LABS
IoT Security

CSA : Key Provisions

ENISA

- ENISA shall carry out tasks for the purpose of achieving a high common level of cybersecurity.
  - Develop and implement Union policy and law.
  - Build capacity, through support for the Computer Emergency ResponseTeam (“CERT”) and the national Computer Security Incident Response teams (“CSIRTs”).
  - Support operational cooperation among Member States, Union institutions, bodies, offices, agencies and stakeholders.
  - Support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes.
  - Provide knowledge and information.
  - Raise awareness and education.

RED ALERT LABS
IoT Security

CSA : Key Provisions

ENISA

- **Organisation** of the ENISA is defined in the CSA:
  - ENISA is **composed** of a Management Board, an Executive Board, an Executive Director, an ENISA Advisory Group and a National Liaison Officers Network, which all have their own organization, functions and duties.
  - ENISA needs to comply with various **obligations** (such as transparency and confidentiality) and should manage its **budgets** responsibly
- CSA grants a **permanent** mandate and provides ENISA with more resources and responsibilities

RED ALERT LABS
IoT Security

CSA : Key Provisions

CyberSecurity certification framework

- CSA defines the CyberSecurity certification framework
  - A mechanism to **establish** European cybersecurity **certification schemes** and to attest that the ICT products, services and processes that have been evaluated comply with specified security requirements.
  - **Candidate certification schemes** will be prepared by ENISA and publishes on a dedicated website maintained by ENISA.
  - Security **objectives** that should be achieved by certification schemes have been established by the EUCybersecurity Act.
  - **Assurance levels** range from “basic”, to “substantial” and “high”.
  - Cybersecurity certification shall be **voluntary, unless otherwise specified by law.**

RED ALERT LABS
IoT Security

Ongoing Schemes under the Cybersecurity Act

EUCC

COMMON CRITERIA BASED EUROPEAN CANDIDATE CYBERSECURITY CERTIFICATION SCHEME

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

EUCS

EUROPEAN CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES

Objective : cloud services cybersecurity certification

5G

Under development

enisa

Potential Future Certification Schemes in the URWP

- **IoT Certification**
  Certification for IoT Devices
- **IACS Certification**
  Certification for Industrial Automation and Control Systems
- **AI Certification**
  Certification for Artificial Intelligence applications
- **Crypto Certification**
  Certification for Cryptographic Modules / or just the crypto stack to be used by EUCC in composition for instance
- **FITCEM Certification**
  Fixed-Time Certification - EN 17640
- **PASSI Certification**
  Certification for Information Systems (Pushed by ANSSI)
- **SDLC Certification**
  Certification for Secure Development Lifecycle processes (Pushed by ANSSI)

RED ALERT LABS
IoT Security

Other obligations of the CS

Mandatory Compliance with the EU Cybersecurity Act

Mandatory Compliance

The EU Cybersecurity Act allow the Commision to enforce compliance to a certain certification scheme

Certification Schemes

While the Act requires certification schemes, actual certification is voluntary unless mandated by other EU laws or regulations.

Mandatory Compliance for Chosen Certification

Once a certification scheme is chosen, compliance with its specific requirements becomes mandatory.

RED ALERT LABS
IoT Security

Penalties for Non-Compliance with EU Cybersecurity Act

EU Cybersecurity Act Penalties

Penalties for non-compliance vary based on specific circumstances and can include legal and financial repercussions under national laws.

Certification Schemes

Failing to adhere to certification schemes or falsely claiming certification can lead to the loss of certifications, legal liabilities, and reputational damage affecting competitiveness in the EU market.

Member State Responsibilities

Member States shall lay down the rules on penalties applicable and take all measures necessary to ensure they are implemented. The penalties shall be effective, proportionate and dissuasive.

Compliance with the EU Cybersecurity Act is crucial to avoid significant legal, financial, and reputational consequences for businesses operating within the EU market.

CSA - Subsection 4

Certification activity

Wording and definitions

Bodies

Conformity assessment Body - CAB

Body that carries out conformity tests (of products, systems, services, people ...)
(e.g. certification body/CB, ITSEF, inspection body)

Certification Body - CB

Third-party conformity assessment body operating certification schemes (ISO/IEC 17065).

The CB is in charge of the activities of certification related to the issuance of certificates;

Activities related to evaluation and testing are performed by the ITSEF (see associated definition).

Under provisions of CSA Art. 58(4), a NCCA can act as a CB. The term CB applies then to both a private CAB and a NCCA acting as a CB.

IT Security Evaluation Facilitiy - ITSEF

Third-party conformity assessment body that performs one or more of the following activities: calibration ; testing ; sampling (adopted from ISO/IEC 17025).

ITSEF is equivalent to Testing laboratory/Evaluation facility. It can be
a) internal to a CAB, or
b) an external entity to which the CAB acting as a CB subcontracts the evaluation.

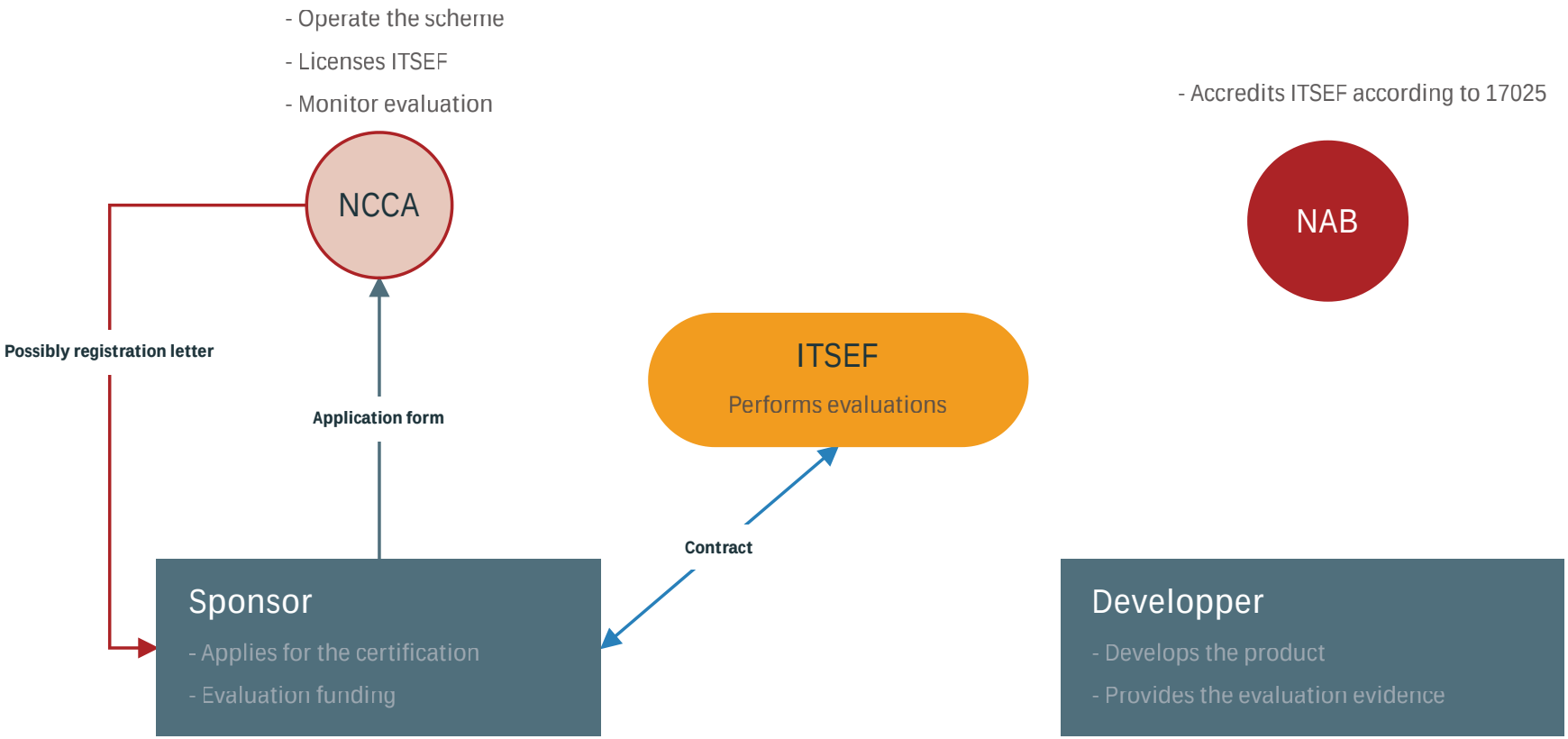
Where requirements are defined in the scheme for an ITSEF, usualy they shall apply to both the internal and external entities.

In the context of the scheme, most of the time the ITSEF is separated from the CB in terms of operations.

RED ALERT LABS
IoT Security

CERTIFICATION PROJECT MANAGEMENT

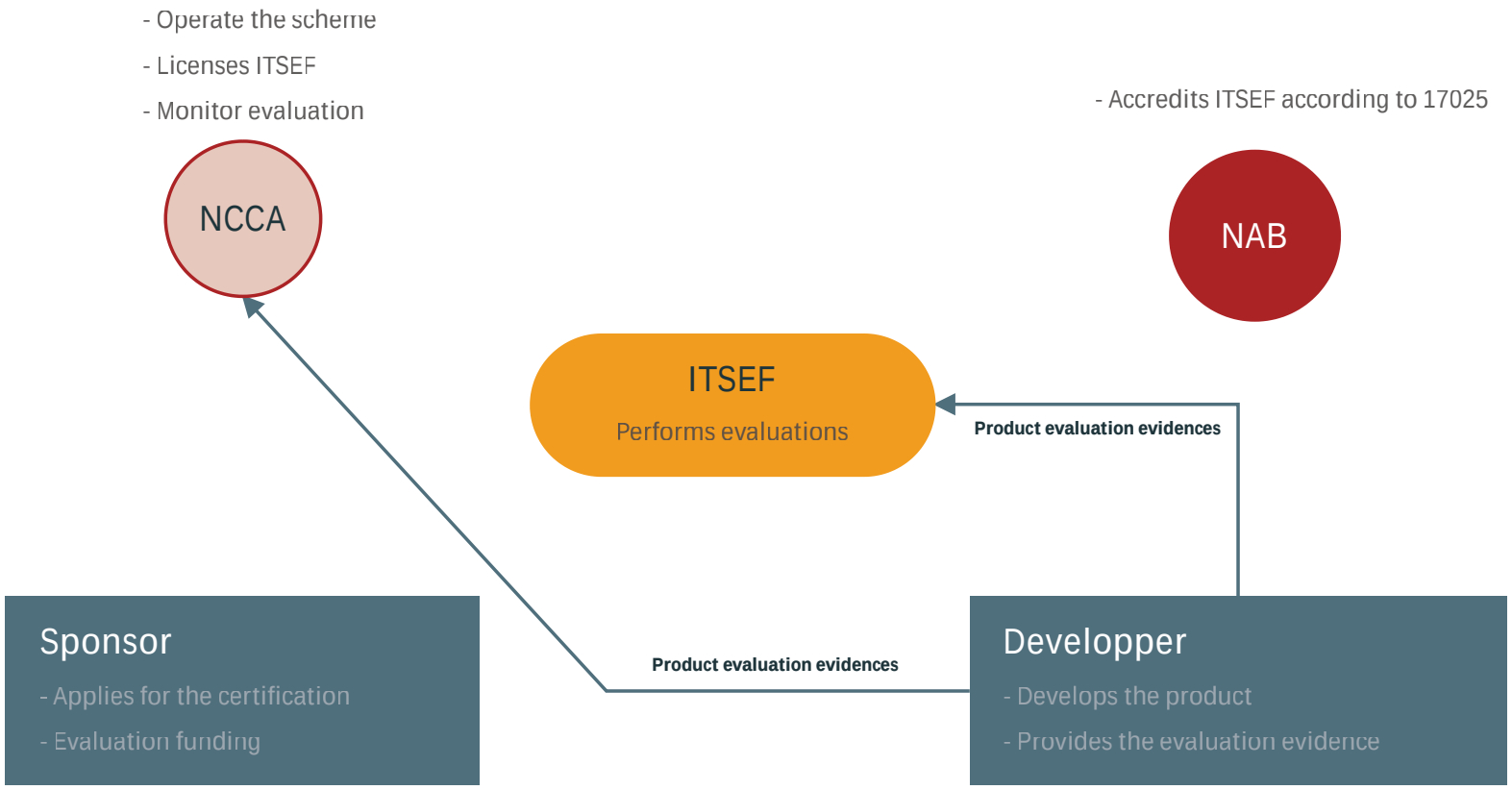
REGISTRATION PROCESS



RED ALERT LABS
IoT Security

CERTIFICATION PROJECT MANAGEMENT

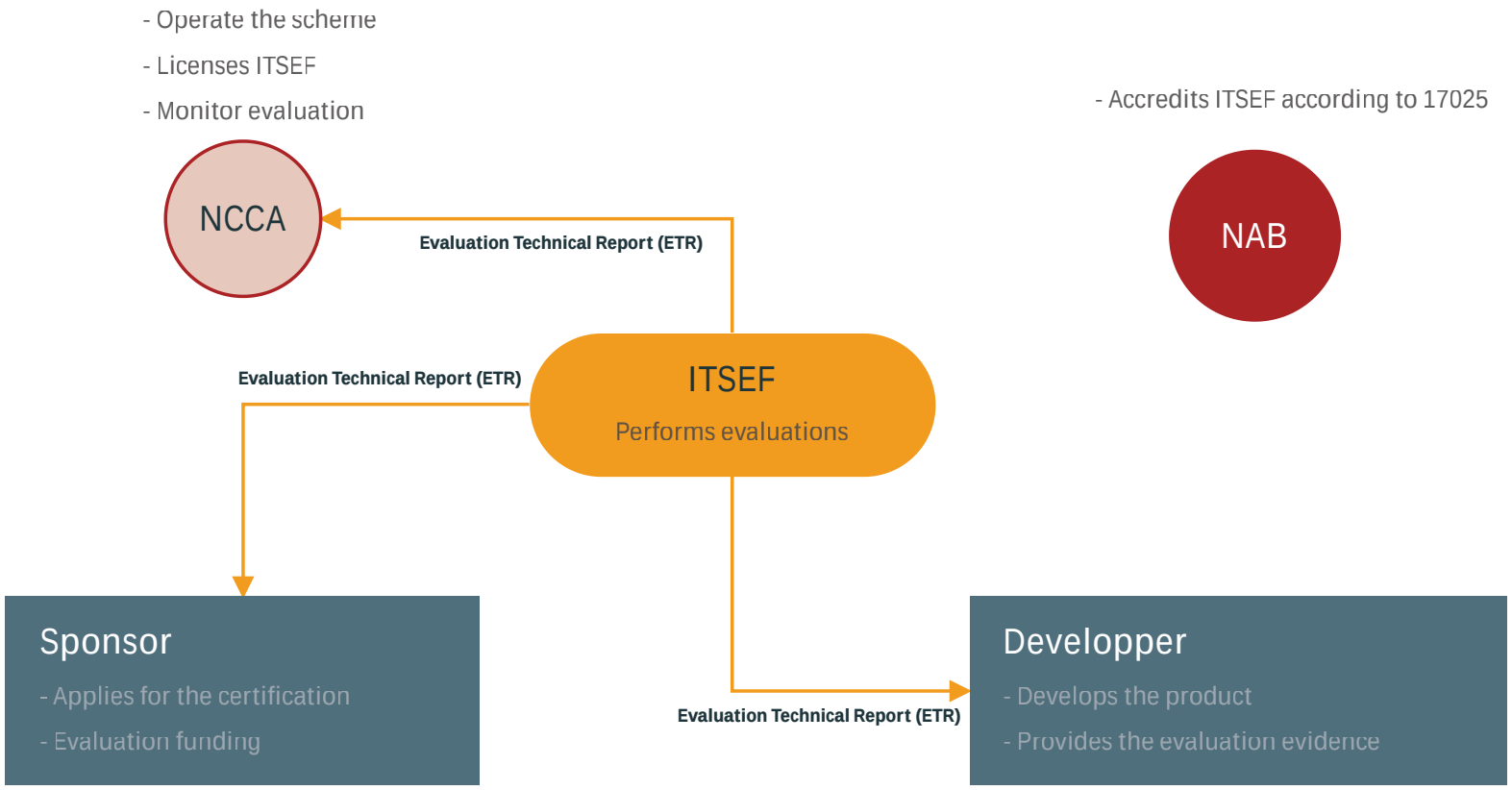
Evaluation process 1/3



RED ALERT LABS
IoT Security

CERTIFICATION PROJECT MANAGEMENT

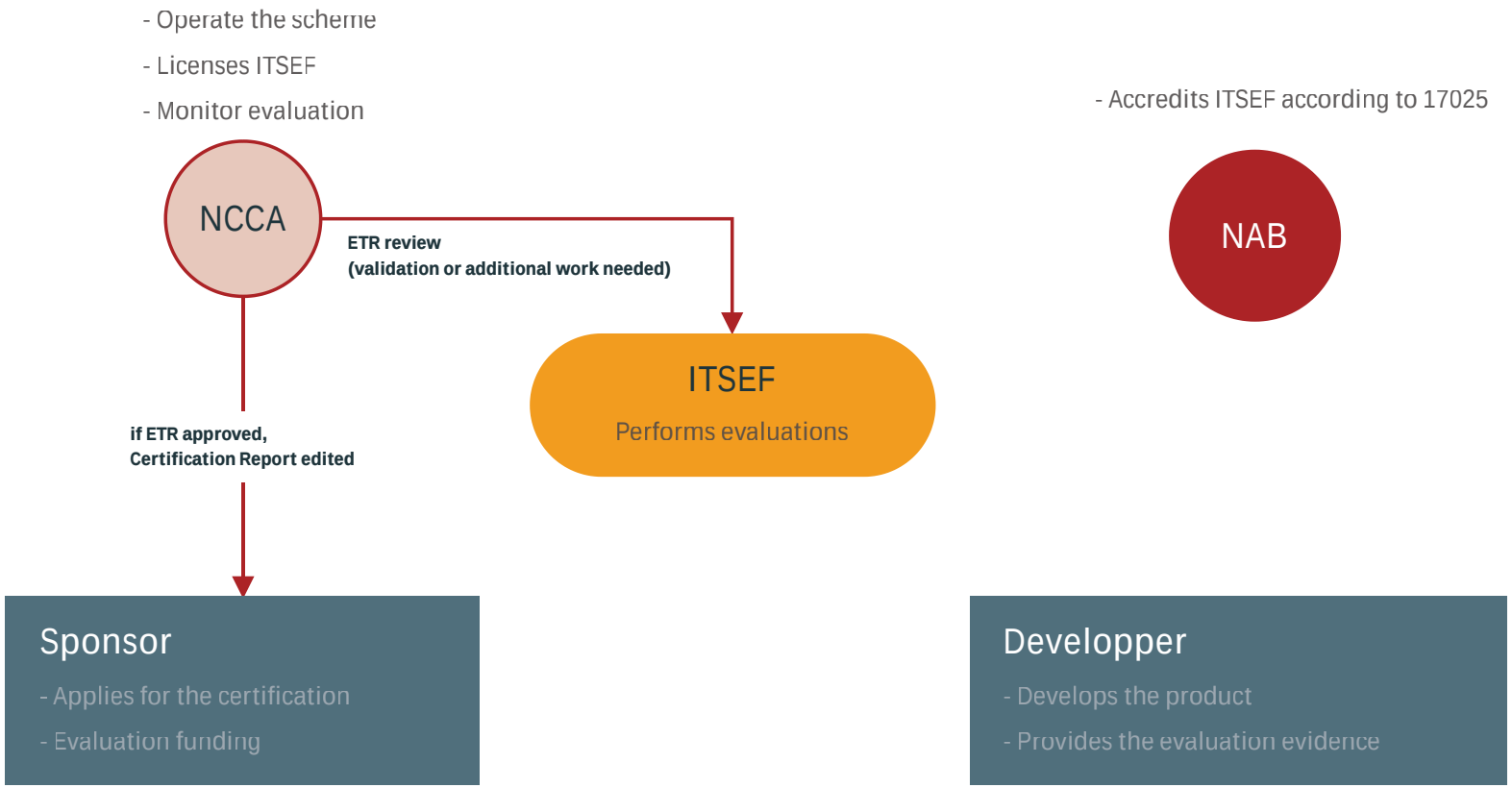
Evaluation process 2/3



RED ALERT LABS
IoT Security

CERTIFICATION PROJECT MANAGEMENT

Evaluation process 3/3



RED ALERT LABS
IoT Security

Wording and definitions

Accreditation vs Authorisation

Accreditation

Accreditation in EU takes place only by the national accreditation bodies (NAB) and is, in accordance with ISO / IEC 17011: 2018-03, a confirmation that a conformity assessment body has the expertise to carry out specific conformity assessment tasks.

Authorisation

Authorisationis granted to examine additional requirements for the technical competence. These possible requirements are schema-specific. If there are no requirements for this in the relevant EU scheme, then there is no authorisation (Article 54.1(f) of CSA).

RED ALERT LABS
IoT Security

Certification Actors

Before CSA - Major trend

- Operate the scheme
- Licenses ITSEF
- Monitor evaluation

NCCA

- Accredits ITSEF according to 17025

NAB

ITSEF

Performs evaluations

Sponsor

- Applies for the certification
- Evaluation funding

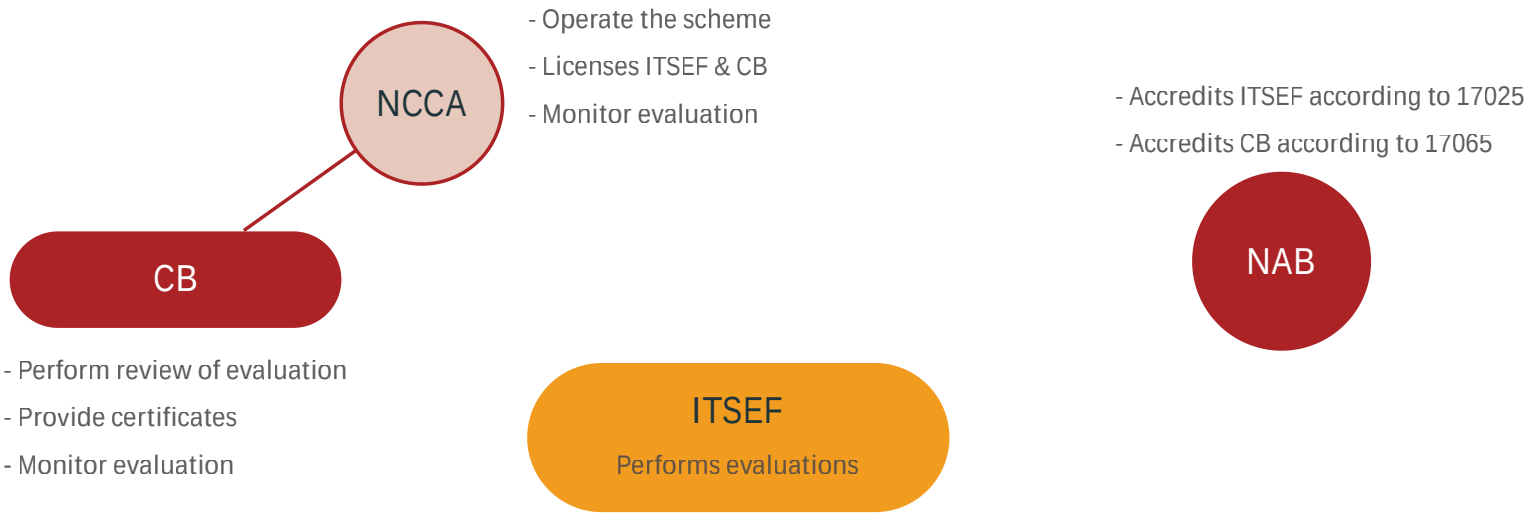
Developper

- Develops the product
- Provides the evaluation evidence

RED ALERT LABS
IoT Security

Certification Actors

After CSA



Sponsor

- Applies for the certification
- Evaluation funding

Developper

- Develops the product
- Provides the evaluation evidence

RED ALERT LABS
IoT Security

NCCA as a CB and ITSEF

Global trend

Before CSA

NCCA as a CB is accredited by NAB(optional) and recognises itself ITSEFs for its own scheme

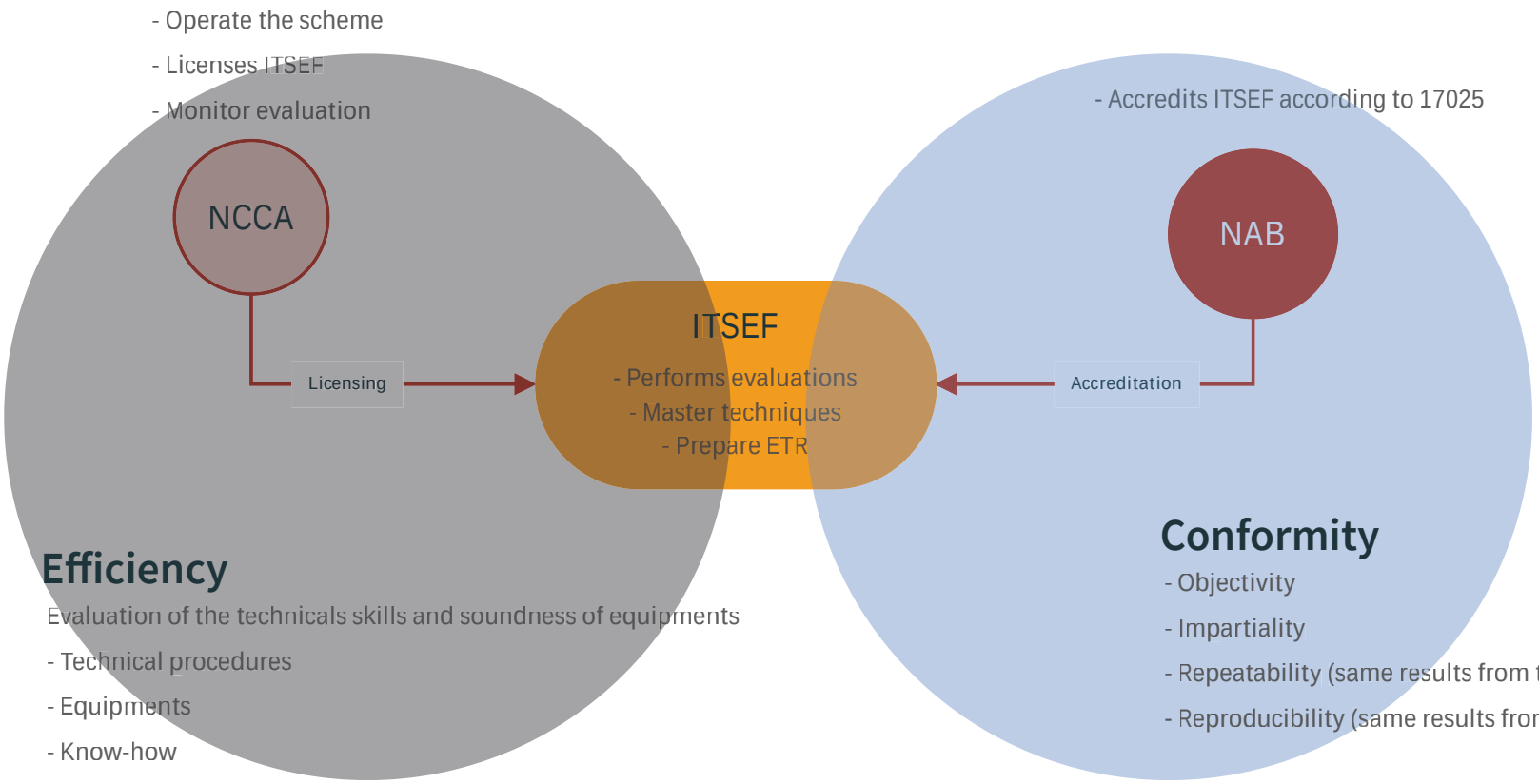
Post CSA

- NAB will accredit CABs (= CBs and/or ITSEFs) for a schemes.
- NCCA will support accreditation and carry out authorisation of CABs.
- CABs need an accreditation of NAB and an authorisation of NCCA.
- Active support of the NAB by the NCCA in monitoring and supervising the activities of the conformity assessment bodies

RED ALERT LABS
IoT Security

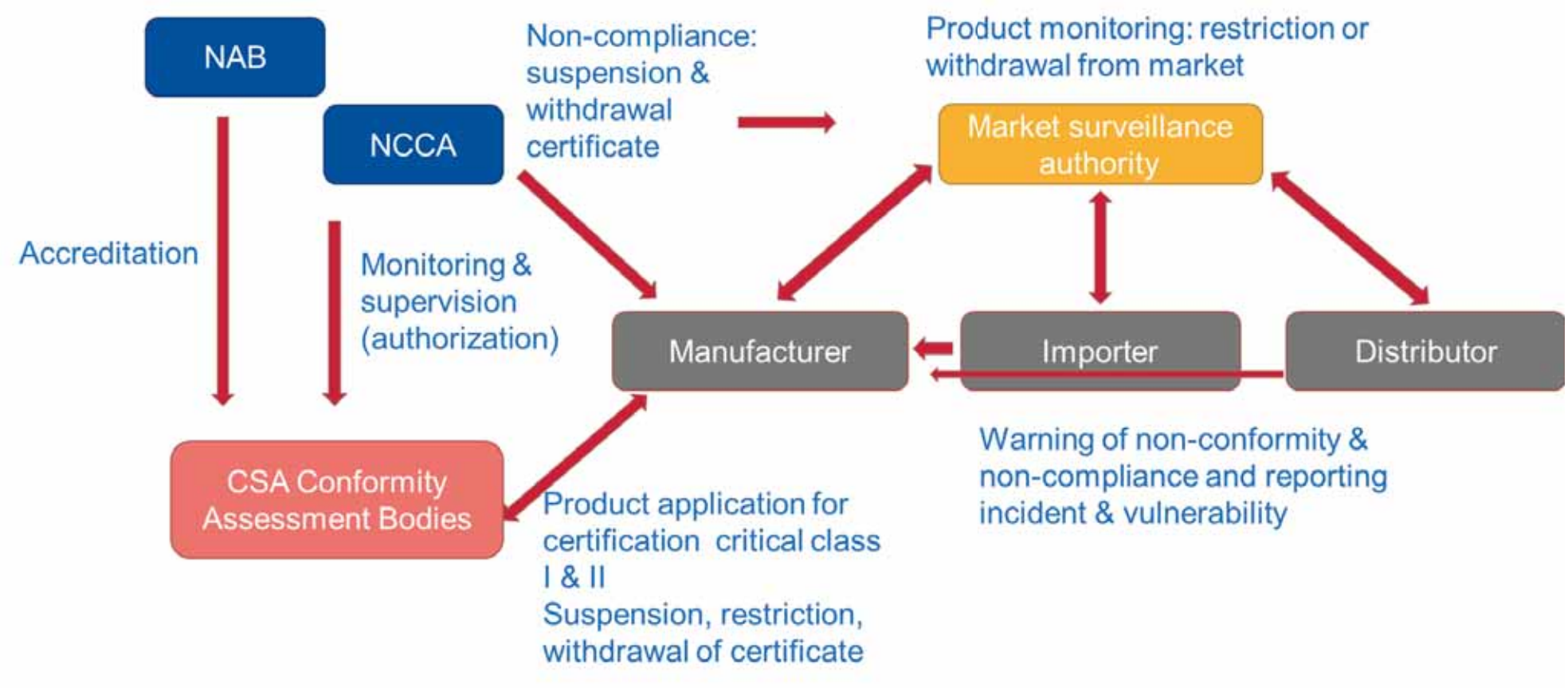
Accreditation vs Authorisation

CERTIFICATION PROJECT MANAGEMENT



RED ALERT LABS
IoT Security

Potential Governance of Schemes under the CSA



CSA - Subsection 2

Zoom on interessting articles for NCCA

CSA - Article 56

Cybersecurity certification

4 | Conformity assessment bodies (CAB) (Art. 60) issue European cybersecurity certificates (Art. 60) of assurance level ‘basic’ or ‘substantial’, based on criteria in the Commission's scheme (Art. 49).

5 | In justified cases, European cybersecurity certificates may be issued by a public body as specified in paragraph 4. Such body shall be one of the following:

- a. a NCCA as referred to in Article 58(1); or
- b. a public body that is accredited as a CAB pursuant to Article 60(1).

6 | Article 49 requires EU cybersecurity certificates with assurance level 'high' to be issued by NCCA or, in certain cases, CABs.

- a. upon prior approval by the NCCA for each individual European cybersecurity certificate issued by a CAB; or
- Delegation to a CAB by the NCCA to issue European cybersecurity certificates.

7 | Submitting party of ICT products/services/processes must provide necessary info to NCCA (if issuing European cybersecurity certificate) or the CAB.

8 | The holder of a European cybersecurity certificate must inform the relevant authority or body of any subsequently detected vulnerabilities or irregularities that may affect its certification requirements.

RED ALERT LABS
IoT Security

CSA - Article 58

National Cybersecurity Certification Authorities

1. Each MS shall designate one or more NCCA in its territory, or, with agreement of another MS, designate authorities from that other state for supervisory tasks.
2. MS shall inform Commission of designated NCCA(s) & assigned tasks of each authorities (if multiple).
3. Each CA shall be independent of entities it supervises in organisation, funding, legal structure, and decisions, per Article 56(5) and 56(6).
4. MS shall ensure activities of NCCAs related to issuance of European cybersecurity certificates are strictly separated from their supervisory activities and independently carried out.
5. MS provides resources to NCCA for proper exercise of powers & tasks.
6. NCCA should actively, effectively, efficiently and securely participate in ECCG for effective implementation of this Regulation.

RED ALERT LABS
IoT Security

National Cybersecurity Certification Authorities shall :

a. Supervise/enforce rules of European cyber certification schemes (Article 54(1)(j)) to monitor ICT product/service/process compliance with European cyber certificates, in cooperation with other relevant market surveillance authorities.

b. Monitor and enforce obligations of ICT product/service/process providers in their territories who conduct **self-assessment** and comply with Article 53(2) & (3) and the relevant European cybersecurity certification scheme.

c. Assist & support National accreditation bodies (NAB) in monitoring and supervising activities of conformity assessment bodies.

d. Monitor and supervise the activities of the public bodies referred to in Article 56(5);

e. Authorise/restrict/suspend/withdraw conformity assessment bodies

f. Handle complaints related to E.U. "High" cyber certificates and self-statements of conformity; investigate, inform of progress/outcome within reasonable time.

g. Provide annual summary report to ENISA & ECCG on activities under (b), (c) & (d) of this § or §8.

h. Cooperate with other authorities (e.g. cert. authorities, public bodies) to share information on possible non-compliance of ICT prod./serv./proc. with this Regulation/specific EU cybersecurity cert. schemes.

i. monitor relevant developments in the field of cybersecurity certification.

RED ALERT LABS
IoT Security

CSA - Article 58

National Cybersecurity Certification Authorities

8 | NCCAs shall have this powers:

a. Request info from assessments bodies, certificates' holders and conformity issuers for tasks.

b. Carry out audits of conformity assessment bodies, EU cybersecurity certificates holders, and issuers of EU statements of conformity to verify compliance.

c. Ensure CABs, certificates' holders and issuers of EU statements of conformity comply with this Reg. or a European cybersecurity certification scheme.

d. Obtain access to premises of CABs or holders of European cybersecurity certificates for investigations under Union/Member State law.

e. Withdraw European cybersecurity certificates issued by NCCA/CAB if they don't comply with the Regulation or Certification Scheme.

f. Impose penalties, as provided in article 65, and require immediate cessation of infringement.

9 | NCCAs shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services and ICT processes.

RED ALERT LABS
IoT Security

CSA - Article 59

Peer review

1 To make sure that European cybersecurity certificates and EU statements of conformity are the same everywhere in the Union, the NCCAs who check them will be checked by others to make sure they're doing their job properly.

3 Peer review shall assess:

a. where applicable, whether the activities of the NCCAs that relate to the issuance certificates are strictly separated from their supervisory activities and whether those activities are carried out independently from each other;

4 Peer review shall be carried out by at least two NCCAs of other MS and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review.

RED ALERT LABS
IoT Security

CSA - Article 61

Notification

1 For each European cybersecurity certification scheme, the NCCAs shall notify the Commission of the CABs that have been accredited and, where applicable, authorised pursuant to Article 60(3) to issue European cybersecurity certificates at specified assurance levels as referred to in Article 52.

The NCCAs shall notify the Commission of any subsequent changes without undue delay.

4 A NCCA may submit to the Commission a request to remove a CAB notified by that authority from the list referred to in paragraph 2.

The Commission shall publish the corresponding amendments to that list in the Official Journal of the European Union within one month of the date of receipt of the NCCA's request.

RED ALERT LABS
IoT Security

CSA - Annex

6 If a CAB is **owned or operated by a public entity** or institution, the independence and absence of any conflict of interest shall be ensured between the NCCA and the CAB, and shall be documented.

RED ALERT LABS
IoT Security

CSA - Subsection 3

Organisational and structural separation

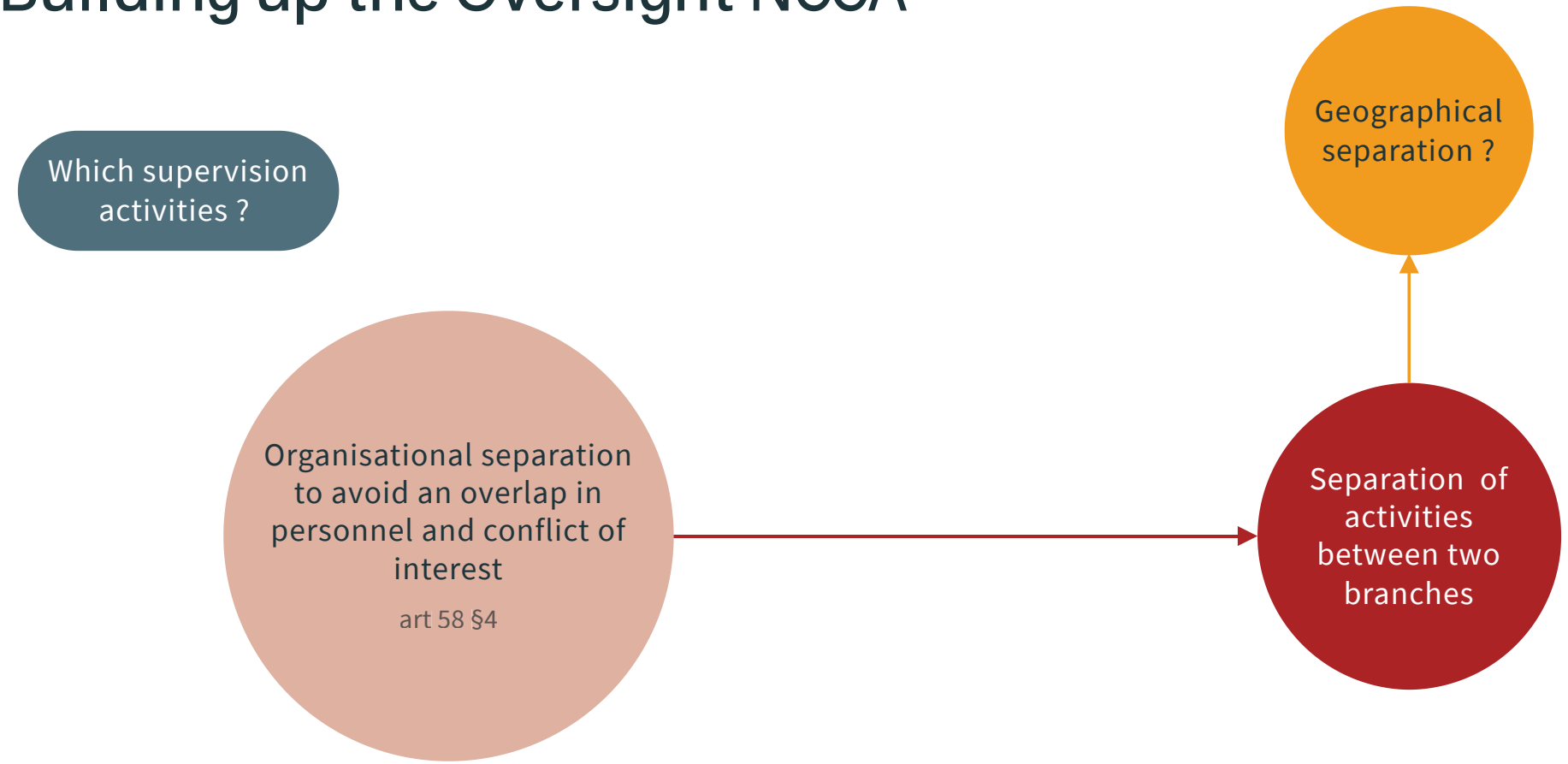
Supervision activities, what does this imply ?

NCCA Implementation of the CSA

	New Circumstances and Obligations				
Authorises CABs	Supervision of conformity self-assesment	Supervision of Certificates by private CAB	Supervision of private CABs	National coordination of European Schemes	Cooperation NAB
Peer Audits on implementation of CSA	National Penalty and Fine Office	Monitoring of NCCA certificates throughout lifecycle	Obligation to report vulnerabilities	Many aspect regulated centrally in EU (like Validity)	ENISA runs Website with certificates

RED ALERT LABS
IoT Security

Building up the Oversight NCCA



RED ALERT LABS
IoT Security

Example of a separation by a European NCCA

Branch 1 - Supervision

NCCA with oversight powers

- Supervision
- Monitoring
- Support NAB
- Complaints and penalties

Branch 2 - Certification 1

Public certification Body (NCCA) - Level high

- EUCC
- EUCS

Branch 3 - Certification 2

Public certification Body (NCCA) - Future Schemes - Level high

- 5G
- etc...

RED ALERT LABS
IoT Security

Example 1 of a separation by a European NCCA

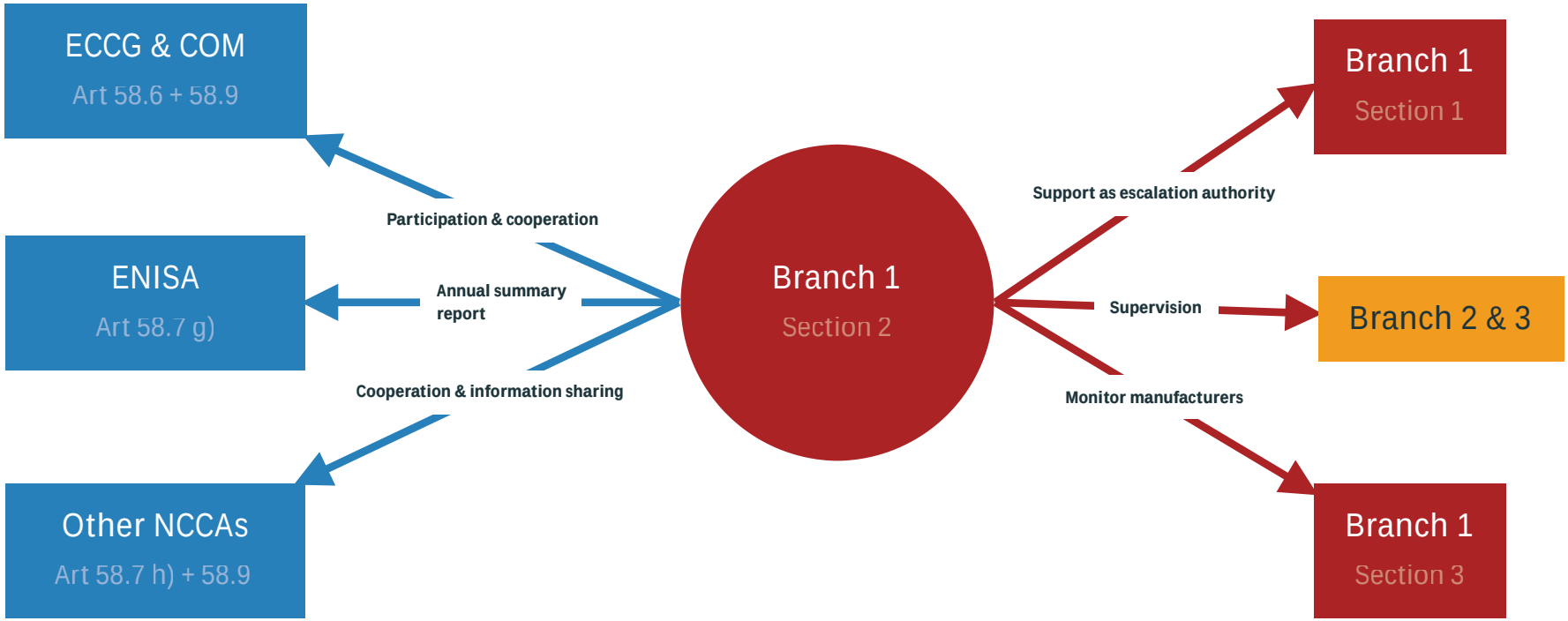
Branch 1 - Obligation as per art 58 § 7.

Section 1 (delegation to CB)	Section 2 (high + ...)	Section 3 (self assessment)
c) actively assist and support the national accreditation bodies in the monitoring and supervision	a) Supervise and enforce rules included in European cybersecurity certification schemes	b) monitor compliance of the manufacturers or providers that carry out conformity self-assessment and are established in the NCCA's territory
	d) Monitor and supervise the activities of the public bodies issuing certificates (NCCA or accredited CB)	
e) authorise conformity assessment bodies and restrict, suspend or withdraw existing authorization where conformity assessment bodies infringe the requirements	f) handle complaints by natural or legal persons in relation to European cybersecurity certificates	
	also paragraphs g), h), i) (annual report to ENISA and ECCG ; inter NCCA cooperation ; monitor development of cybersecurity certification)	

RED ALERT LABS
IoT Security

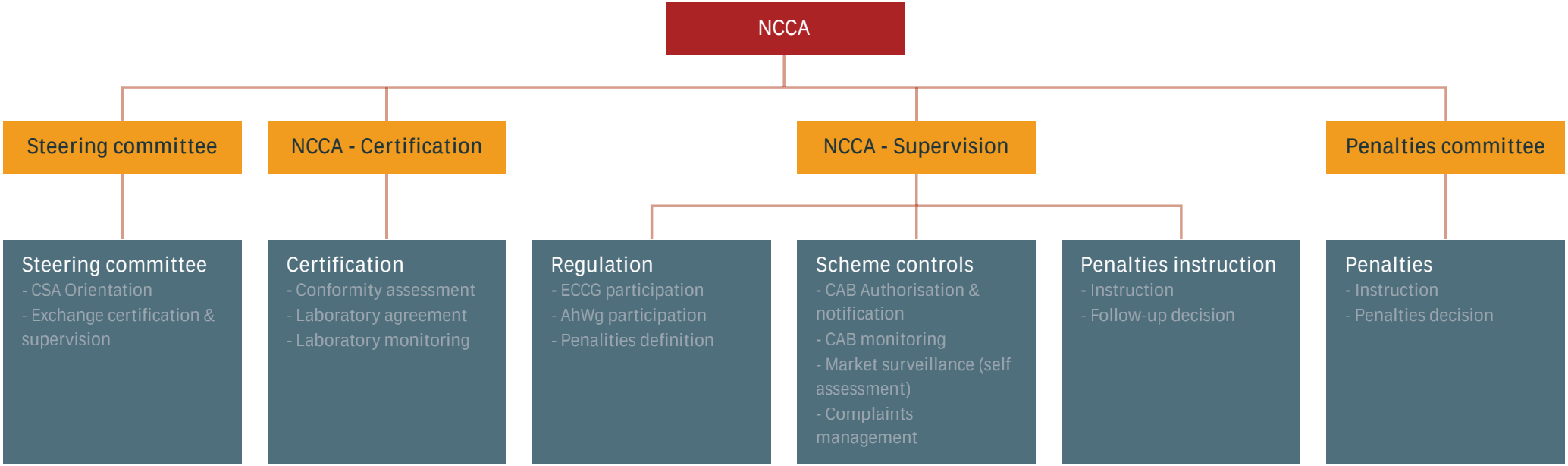
Example 1 of a separation by a European NCCA

Branch 1 - Section 2 – interactions of section 2



RED ALERT LABS
IoT Security

Example 2 of a separation by a European NCCA



RED ALERT LABS
IoT Security

CSA

Questions - Segregation of NCCA supervision and NCCA certification

According to EU Regulation 2019/881 Article 59.3(a)

==> Peer review shall assess where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other;

- Is it sufficient to have NCCA (supervision) as a different department as NCCA (certification) within the same Administration or Ministry?

Questions

RED ALERT LABS
IoT Security

Answers

- Is it sufficient to have NCCA (supervision) as a different department as NCCA (certification) within the same Administration or Ministry?

  Some countries prefer to separate these two entities geographically.

  Nevertheless having the NCCA supervision and certification functions within the same administration or ministry may be possible, it is important to ensure that there are clear separation of powers, decision-making processes, and that the NCCA has the necessary legal basis, independence, resources, and oversight to carry out its functions effectively and with integrity.

RED ALERT LABS
IoT Security

CSA

NCCA Supervision activities

Check note

Key Activities

Which points are important to retain?

8 POINTS

1. CAB authorisation & notification
   Art 58.7.e) + Art 61.1
2. CAB monitoring
   Art 58.7.c) + Art 58.7.d)
3. Manufacturer & provider monitoring
   Art 58.7.b)
4. Complaints management
   Art 58.7.f) + Art 63
5. Penalties management
   Art 58.8.f)
6. Registration of statement of conformity (and certificates)
   Art 53.3
7. Vulnerability management
   Art 55.1.d) + Art 56.8 + Art 58.7.h) + Scheme requirements
8. Support to NAB for the accreditation of CABs
   Not directly linked to a requirement

RED ALERT LABS
IoT Security

CSA

Questions

List of policies, procedures and forms to cover NCCA activity

- What are the documents required for a NCCA in order to cover all its activity?

Questions

RED ALERT LABS
IoT Security

Answers

- What are the documents required for a NCCA in order to cover all its activity?

  There is no explicit list of document required, it is more about processes to cover.

  Slide “NCCA Supervision activities - key activities” explicits these.

- Here is an example of potential types of documentation ==>

RED ALERT LABS
IoT Security

Potential Types of Documentation

- **Certification Framework Documentation**
  Detailed guidelines and procedures for implementing the EU cybersecurity certification schemes, covering ICT products, services, and processes. These documents would include criteria for assessing conformity to specified security requirements.
- **Compliance Monitoring Procedures**
  Documents outlining the methods and processes for monitoring compliance with the obligations set by the cybersecurity certification schemes, including those related to self-assessment by manufacturers or providers.
- **Complaint Handling Procedures**
  Guidelines and procedures for receiving, investigating, and resolving complaints related to European cybersecurity certificates or EU statements of conformity.
- **Cooperation and Information Sharing Protocols**
  Procedures for cooperating with other national cybersecurity certification authorities, public authorities, and possibly ENISA, including mechanisms for sharing information about non-compliance or cybersecurity threats.
- **Personnel and Training Records**
  Documentation on the training and expertise of staff involved in the certification and supervision processes, especially those issuing certificates for high assurance levels.
- **Audit and Inspection Reports**
  Records of audits and inspections carried out to verify compliance with cybersecurity certification schemes and to investigate complaints.
- **Certification Issuance and Withdrawal Records**
  Documentation related to the issuance, renewal, and, if necessary, withdrawal of cybersecurity certificates.
- **Public Communications**
  Guidelines for making necessary information publicly available, including guidance for end-users on securing certified ICT products, services, and processes.
- **Data Protection and Security Policies**
  Given the sensitive nature of the information handled by NCCAs, comprehensive data protection and security policies are essential to protect personal data and classified information in line with EU regulations.

RED ALERT LABS
IoT Security


Coffee
break

Cyber Resilience Act (CRA)

Agenda

1 | CSA

1. Context
2. Introduction
3. Certification Activities
4. Impact of the CSA on NCCA's missions

2 | CRA

1. Context
2. Scope
3. Main Requirements
4. CSA vs CRA

RED ALERT LABS
IoT Security

What is CRA?

European **Cyber Resilience Act** unifies EU cybersecurity rules for more secure hardware and software products. It will help safeguard consumers and businesses buying or using Products with Digital Elements (PDEs).

RED ALERT LABS
IoT Security

“A first legislation of its kind at EU level: the Cyber Resilience Act introduces mandatory cybersecurity requirements for hardware and software products, throughout their life cycle.”

EUROPEAN COMMISSION, SEPT 2022

RED ALERT LABS
IoT Security

What Makes a PDE?

Product Connectivity

A PDE is connected to other devices or networks to exchange data, either through a direct or indirect connection, using physical, wireless/radio, or virtual means.

Remote Data Processing

A PDE includes remote data processing capabilities, allowing for data processing and analysis to be performed outside of the local device.

Market Availability

A PDE is made available in the European Union (EU) market, regardless of where the product has been developed or produced.

Internal Solutions Exclusion

Solutions used for internal purposes, and not made available to the broader market, are not considered PDEs.

In summary, a PDE is a product that has digital elements, is connected to other devices or networks, includes remote data processing, and is made available in the EU market, regardless of its origin.

Products with digital elements

Products and components marketed separately

Such as laptops, smart devices, cell phones, network equipment or CPUs.

Software products and components marketed separately

Such as operating systems, word processors, games or mobile applications.

Remote data processing solutions

Including the definition of products with digital elements.

Products with digital elements are varied, and include hardware and software products, as well as remote data processing solutions.

Cyber Resilience Act (CRA) - Overview

CRA Overview

Addresses growing cybercrime (EUR 5.5 trillion global annual cost by 2021)

Increase Trust & Security

Aims to increase trust, security, and legal certainty in EU digital products

Regulations

Complements existing EU cybersecurity regulations (NIS2, EU CSA)

The CRA Overview is an important initiative to address the growing cybercrime threat and ensure trust, security, and legal certainty in EU digital products.

Cyber Resilience Act (CRA) - Goals

To reduce vulnerabilities in digital products

To ensure cybersecurity is maintained throughout a product's life cycle

To enable users to make informed decisions when selecting and operating digital products

The CRA establishes horizontal mandatory cyber-security requirements for all digital products, software and/or hardware.

What is the scope of the CRA?

Default Products

- 90% of products
- Hard drives
- Smart speakers

Important Products Class I

- Password managers
- Operating Systems
- Wearable devices

Important Products Class II

- Hypervisors
- Firewalls
- Intrusion Detection Systems

Critical Products

- Smartcards
- Hardware Security Modules
- Smart meter gateways

All products with digital elements (PDEs) in the EU market, divided into 4 categories:

Exclusions...

Non-commercial projects

including open-source software, insofar as a project is not part of a commercial activity "earning money beyond maintenance costs."

Services

Services, in particular cloud software/software-as-a-service - with the exception of "remote data processing solutions". Websites that do not support the functionality of a product with digital elements

Sufficiently regulated products

(cars, medical devices, in vitro, certified aeronautical equipment) under the new and old approaches;

Few Components

Exclusion of components manufactured as spare parts for products with digital elements marketed before the date of entry into force of the Regulation.

...skipping a few products crossing the line !

CRA - Fabricants

Main Obligations

- Security By Design and by Default
- Transparency in the supply chain for hardware or software components.
- Vulnerability management for each product.
- Cybersecurity requirements throughout the life of the product/solution
- A list of software components that will be updated regularly (SBOM)
- After-sales support for product security / secure update.
- Transparency (on the security provided, the expected lifespan, etc.) and security support
- Inform the end user about the cybersecurity level of the product.
- Diligence for manufacturers.

RED ALERT LABS
IoT Security

Requirements of CRA

Design and development phase

- ✔ Product risk assessment [art 13(2)]
- ✔ Essential requirements for the product (Annex I, Part 1)
- ✔ Vulnerability Management : Essential requirements (Annex 1, Part 2)
- ✔ technical documentation, including information and instructions (Annex II + VII)
- ✔ Conformity evaluation [article 27]
  - Self assessment **– Module B+C - Module H – EU certificate(Annex VIII)**
- ✔ CE MARKING, Declaration of conformity; (Annex V, VI)

Maintenance phase (5 years minimum product support)

- ✔ Obligation to report to the CSIRT and ENISA
- ✔ Actively exploited vulnerabilities Serious incidents
- Alert Notice: Early alert notification within 24 hours
- Vulnerability notification within 72 hours

Security Update (10 years)

- ✔ Security updates that were made available to users during the support period remain available after release for a minimum period of 10 years or for the remaining duration of the support period, whichever is longer being retained.

RED ALERT LABS
IoT Security

Requirements for Device Economic Operators

Get products certified

- Self assessment
- 3rd party validation
- Certification

Compile Software Bills of Materials (SBOM)

- Define software suppliers
- Define who is responsible of software modules & stages

Ensure security updates

- Define intended purpose and requirements of the product
- Provide security updates over product lifetime

Report product vulnerabilities

- Yet to be defined

For whom is the CRA applicable?

Manufacturers

Entities that produce and deliver PDEs to consumers in the EU market

Providers

Entities that provide components or software (Proprietary and Open Source software) used by manufacturers

Importers

Entities that import or distribute PDEs marketed in the EU

If you're involved in the process of building or delivering a PDE in the EU market, you'll have the expectation to comply with the CRA

CRA main requirements

4 main obligations in the CRA

Risk Assessment

Manufacturers must ensure that products are delivered:

- Without known exploitable vulnerabilities
- Secure by default and with limited attack surface
- Minimizing processing of data

RED ALERT LABS
IoT Security

CRA Main Obligations

Risk Assessment

CRA Requirement	Related Process/Controls
Product with no exploitable vulnerabilities	SDLC, Vulnerability Management, Threat-Led Pentest
Secure By Default	Threat Modelling / Hardening
Limited Attack Surface	Secure Configurations
Protect Data and Minimized Data Processing	Data Protection Impact Assessment

RED ALERT LABS
IoT Security

CRA main requirements

4 main obligations in the CRA

Documentation

Manufacturers must deliver documentation to address:

- Product Design, Delivery and Vulnerability Management
- Risk Assessment and Conformity Declaration
- Software Bill of Materials (SBOM)

RED ALERT LABS
IoT Security

CRA Main Obligations

Documentation

CRA Requirement	Related Process/Controls
Product Design and Development	SDLC defined policy and process
Vulnerability Management	Vulnerability Management policy (reporting,triaging, communication, patching)
Risk Assessment	Threat Modelling
Conformity Declaration	Audit / Attestation reports
Software Bill of Materials (SBOM)	List all components, dependencies and vulnerabilities (human and machine readable)

RED ALERT LABS
IoT Security

CRA main requirements

4 main obligations in the CRA

Conformity Assessment

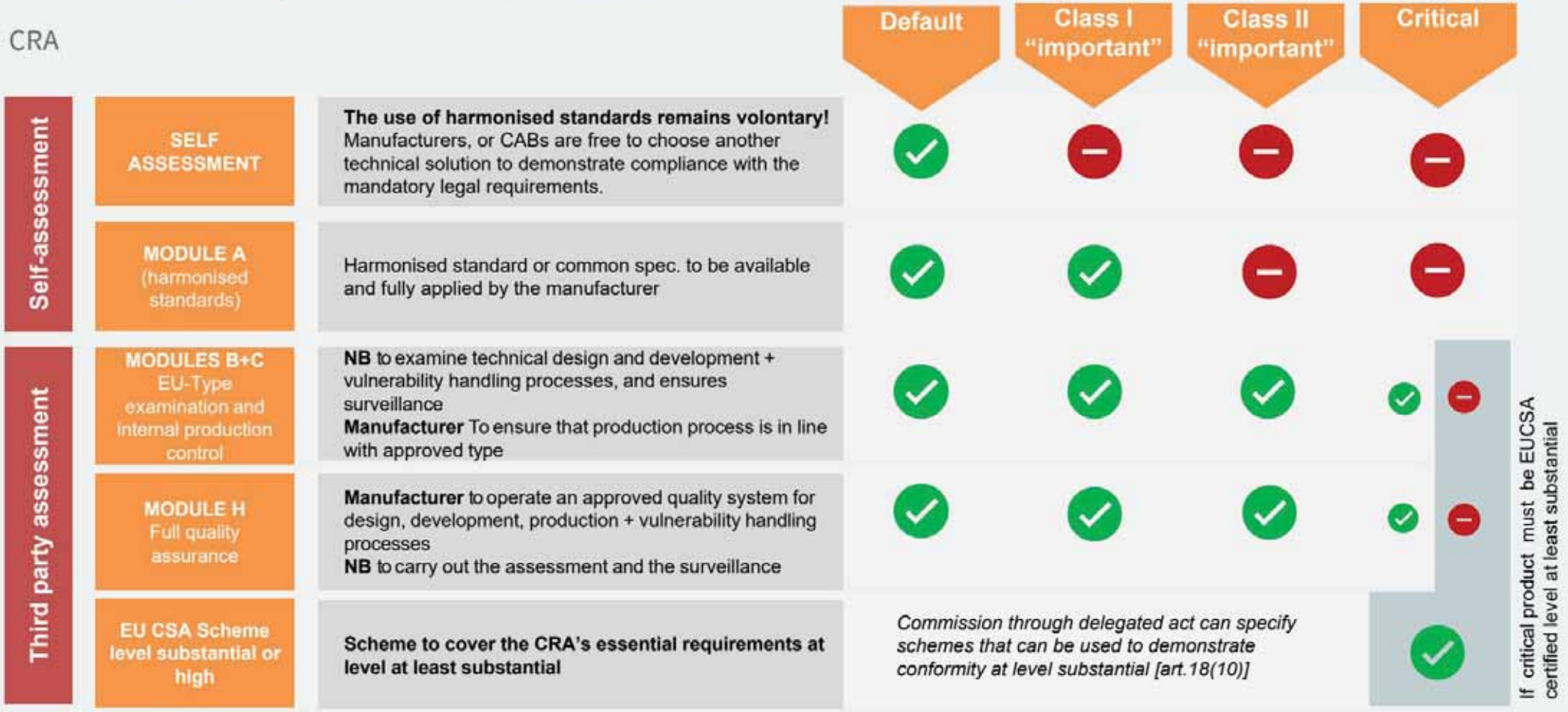
Manufacturers must provide a declaration of conformity:

- Self Assessment
- Provided by independent Third Party Auditor

RED ALERT LABS
IoT Security

Conformity Assessment Procedures

CRA



RED ALERT LABS
IoT Security

CRA main requirements

4 main obligations in the CRA

Vulnerabilty Reporting

Vulnerabilities must be reported to ENISA:

- Actively Exploited Vulnerabilities
- Security Incidents that affect the product
- 24 hours after becoming aware

RED ALERT LABS
IoT Security

CRA Main Obligations

Vulnerabilty Reporting

	CRA Requirement	Related Process/Controls
Report to ENISA within 24 hours of being aware	Actively Exploited Vulnerabilities	Vulnerability Management (Intake, Triaging, Mitigation/Remediation, Communication, Security Updates and patches)
	Security Incidents related to the Product	Incident Response Process (Playbooks, Communication and reporting procedures)

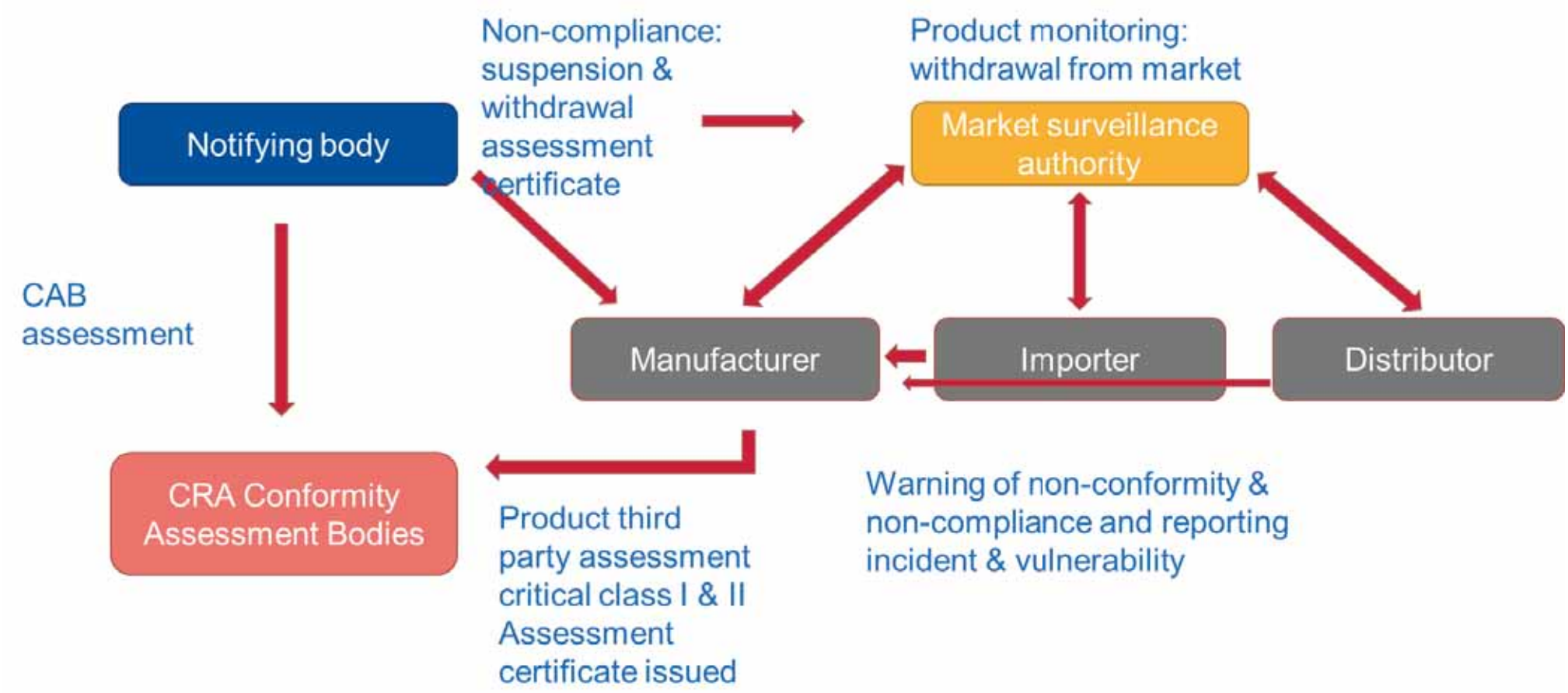
RED ALERT LABS
IoT Security

CSA vs CRA

CSA - Certification
• **Long term life-cycle** ensured • **Composition of certifications** • **Risk based Assurance levels** & corresponding cybersec. requirements (upgrading-down grading) • **Horizontal & sectoral** • **Accreditation & Authorization** of CABs (high) • **Complaints procedures by all actors** in certification (CABs & NCCA) & legal remedy • **Central EU certification** database ENISA • Implementing Regulation has a fallback clause – repair clause if procedures do not work. • No supply chain security & data minimization

CRA - Statement of conformity/assessment certificate
• **Short term lifecycle** - max 5 years • **No building block system** • **"Static" but broad requirements, risk-based** conformity assessment • **Horizontal** • **No accreditation** obligated • **Complaints procedures: not explicitly** described **under CRA** (maybe ruled by use of standards) • **Decentralized:** notified bodies and authorities have the certification information (& status) • **Non-compliance** attributed to shortcoming scheme -> Commission amendment/repeal of implementing Act describing the presumption of conformity (art 18 (4) CRA) • Supply chain security: SBOM & data minimization

CRA Governance



Penalities

€ 15.000.000
2,5 %
Revenue

NON-COMPLIANCE WITH ESSENTIAL REQUIREMENTS AND VIOLATIONS OF SPECIFIED DUTIES

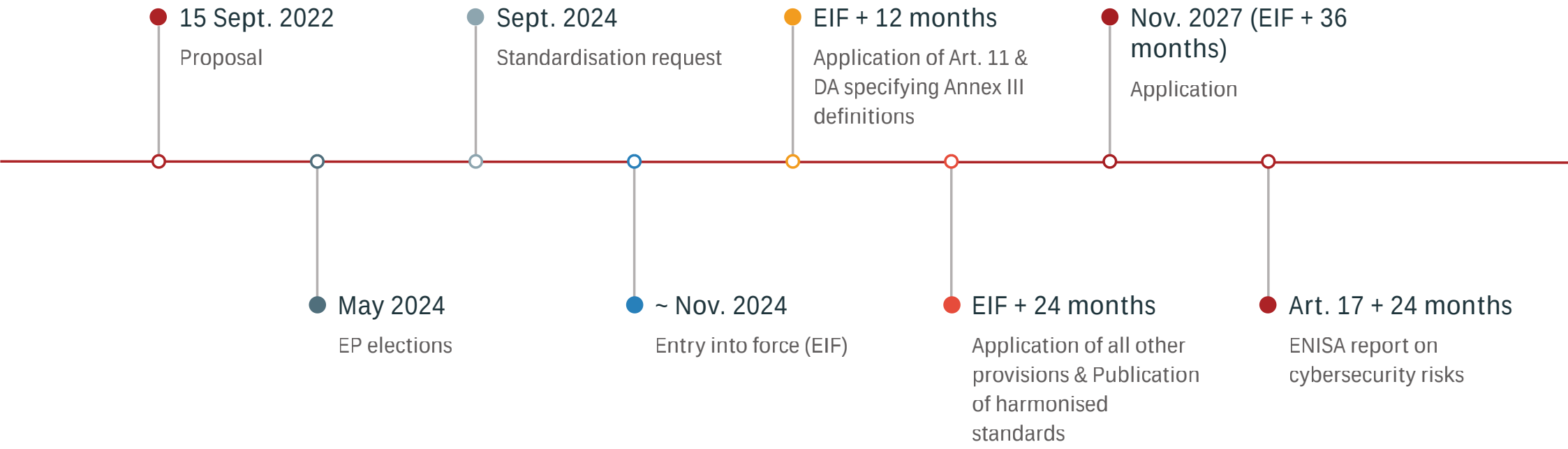
€ 10.000.000
2 %
Revenue

NON-COMPLIANCE WITH OTHER OBLIGATIONS

€ 5.000.000
1 %
Revenue

FALSE, INCOMPLETE OR MISLEADING INFORMATION PROVIDED TO MARKET SURVEILLANCE AUTHORITIES

Tentative Timeline for CRA Regulation



RED ALERT LABS
IoT Security

Questions

- ✔ Question #1

  What are the main obligations imposed by the CRA on manufacturers?

- ✔ Question 2

  How are PDE classified?

RED ALERT LABS
IoT Security

Responses

- Cybersecurity requirements throughout the life of the product/solution + obligation of transparency and security support + An obligation of transparency in the supply chain + A list of software components which will be updated regularly + An obligation of information for the end user on the level of cybersecurity of the product + A duty of care for manufacturers + Vulnerability management for each product.

- Default, Important Class 1, Important Class 2 and Critical

RED ALERT LABS
IoT Security

Let's meet!

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

RED ALERT LABS

IoT Security

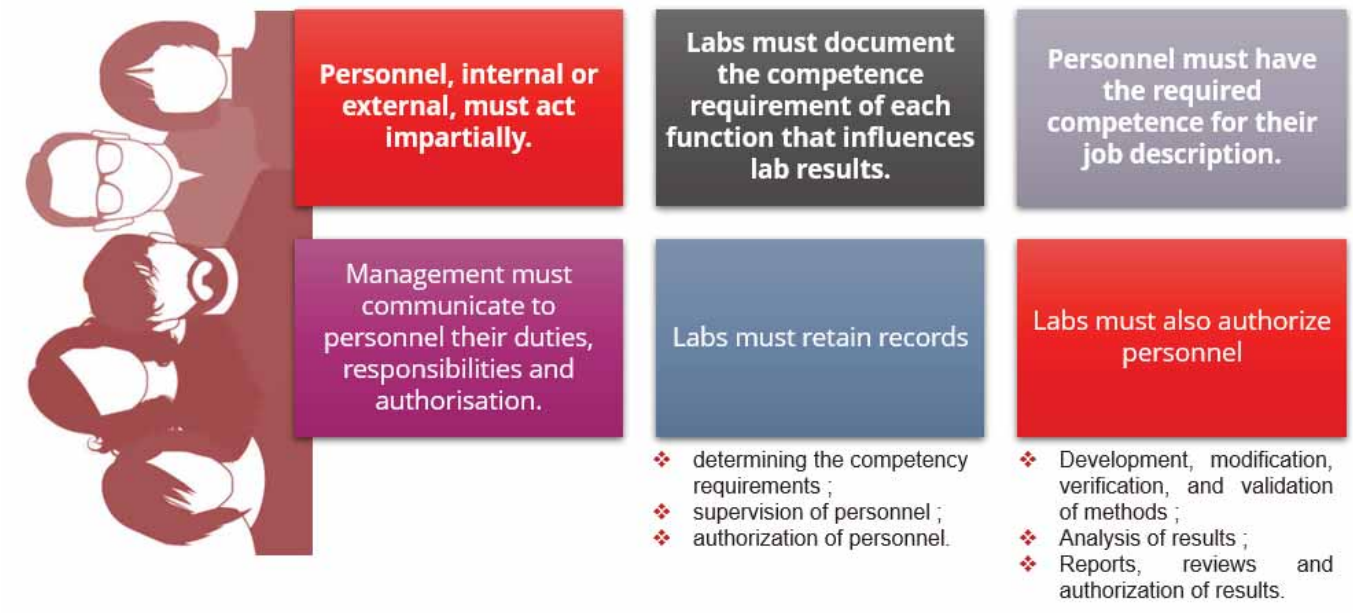
CSA - Subsection 5

Accreditation and Authorisation

Accreditation vs Authorisation

Competences Example

Reminder ISO 17025



Accreditation vs Authorisation

Competences Example

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

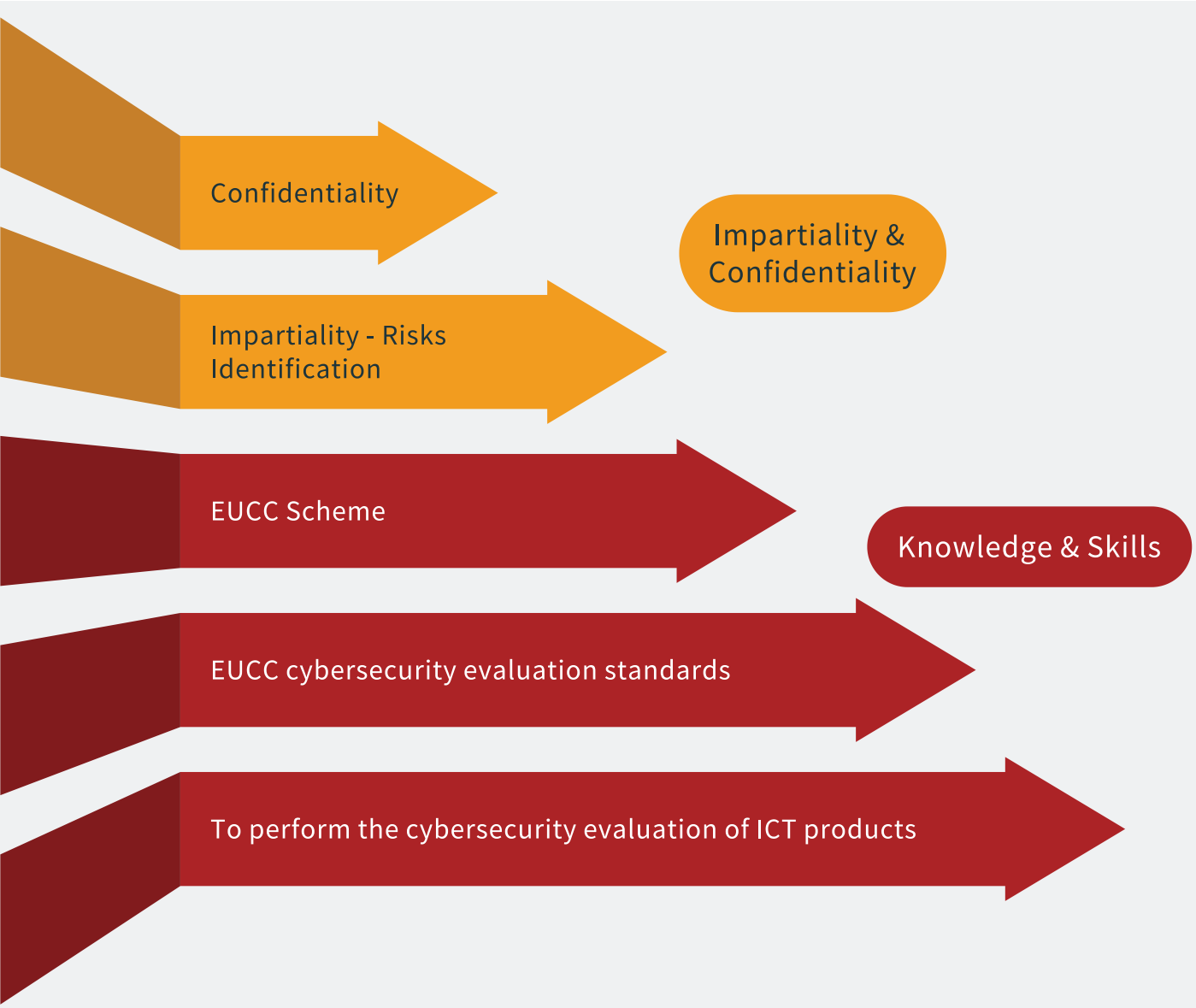
ITSEFs and their evaluators

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

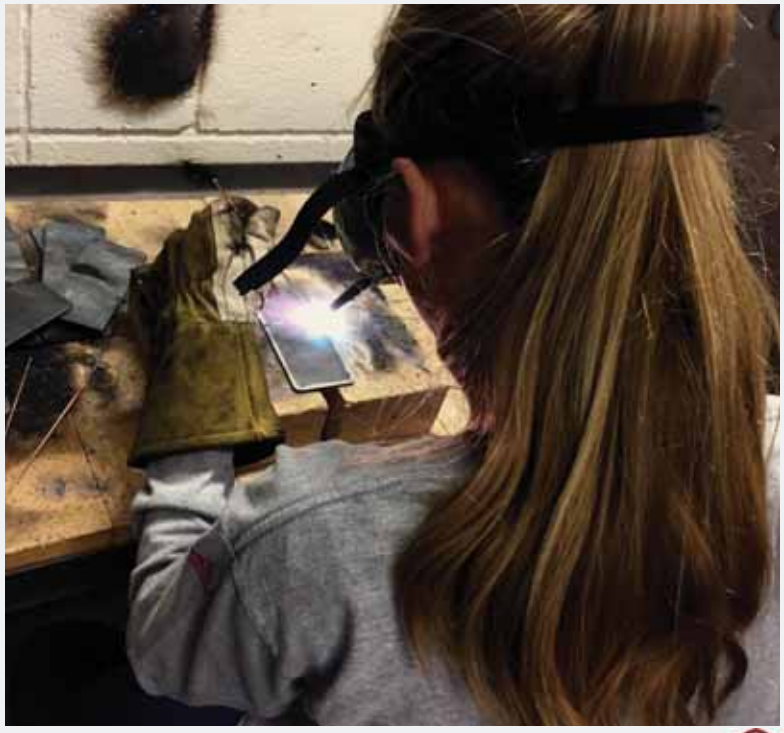
RED ALERT LABS
IoT Security

Accreditation vs Authorisation

Normative Competencies

ISO/IEC 19896-1

- Level 1 - Associate
- Level 2 - Professional
- Level 3 - Manager
- Level 4 - Principal



RED ALERT LABS
IoT Security

Accreditation vs Authorisation

Normative Competencies

ISO/IEC 19896-1

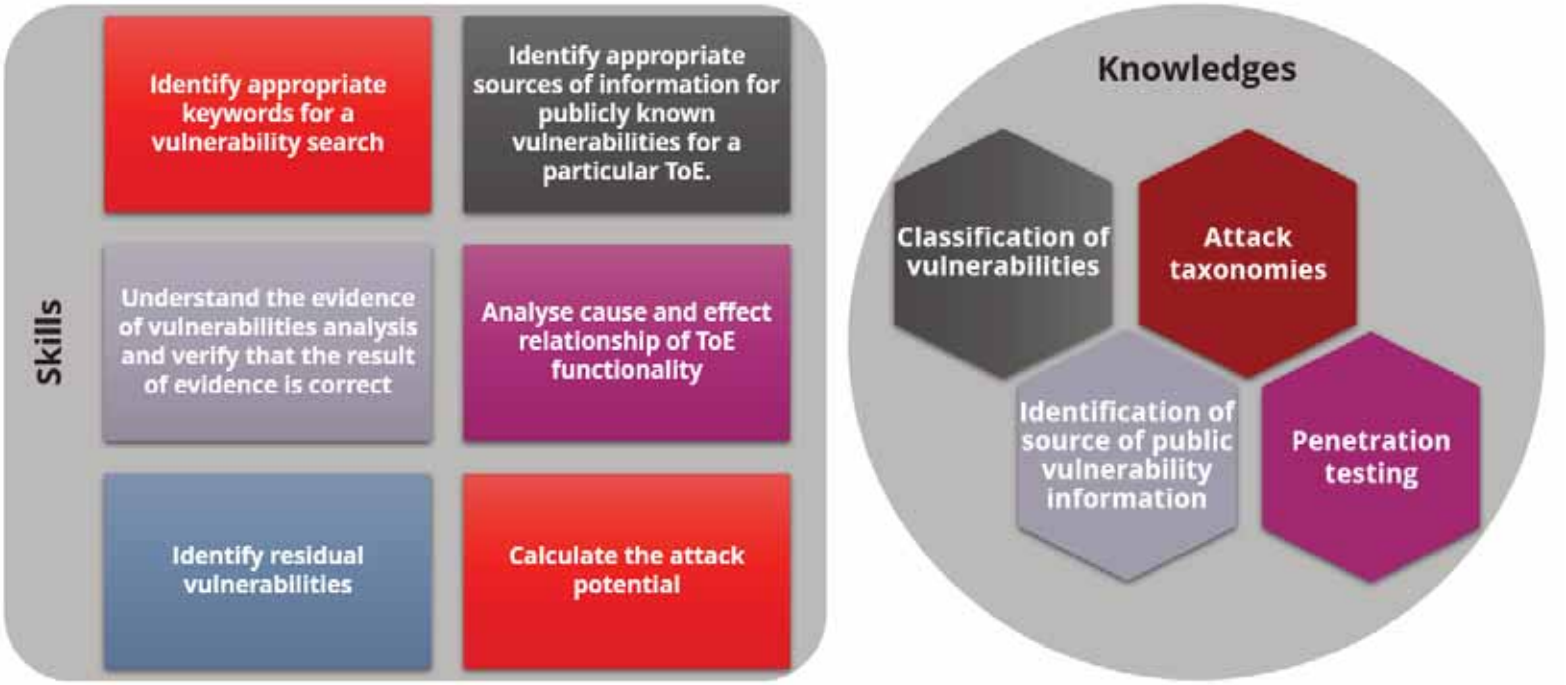
Measurement of elements of competences

- 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

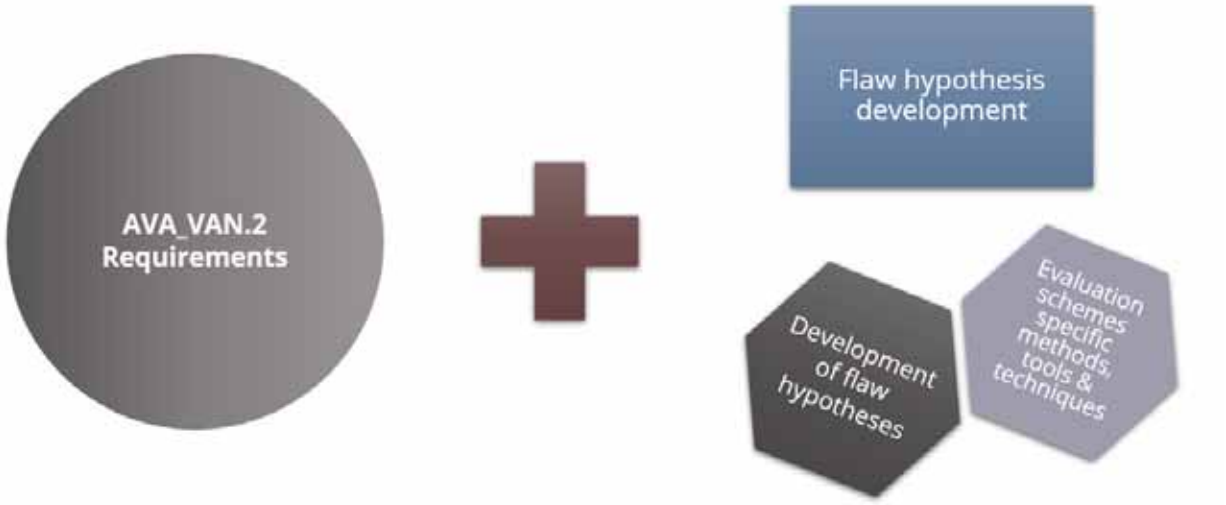
Competences Example

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)



Accreditation vs Authorisation

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

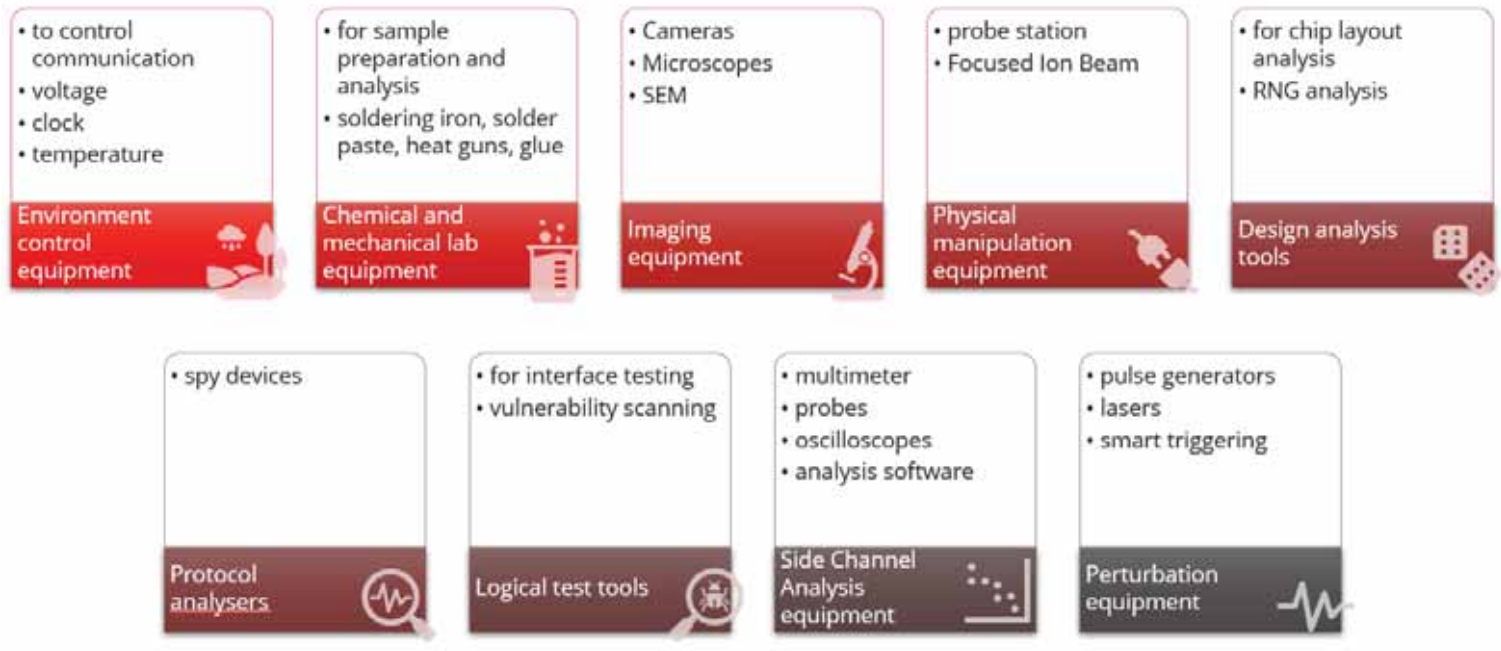
Maintain records about equipment , their location, calibration date, reference materials, equipment repairs, etc

RED ALERT LABS
IoT Security

Accreditation vs Authorisation

Equipment Example

EUCC - Example of required equipment



Accreditation vs Authorisation

Standards to take into account

EUCC ITSEF

To build Lab system management

- **ISO/IEC 17025:2017**

Conformity

To ensure competencies, knowledge and skills

- ISO/IEC 19896-1:2018

- ISO/IEC 19896-3:2018

- ISO/IEC TS 23532-1:2021

- ISO/IEC 15408-1
- ISO/IEC 15408-2
- ISO/IEC 15408-3
- ISO/IEC 18045

Efficiency

RED ALERT LABS
IoT Security

Additionnal interesting information related to specific topics