A4CEF

RED ALERT LABS
IoT Security

INTRODUCTION TO CERTIFICATION AND EU CYBERSECURITY ACT

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

AGENDA DAY 1

1. Introduction to ICT Certifications

- History
- Types
- Scope
- Next Steps

2. EU Cybersecurity Act

- Definition
- History
- ENISA Mandate & Objectives
- Benefits

3. EU Cybersecurity Certification Framework

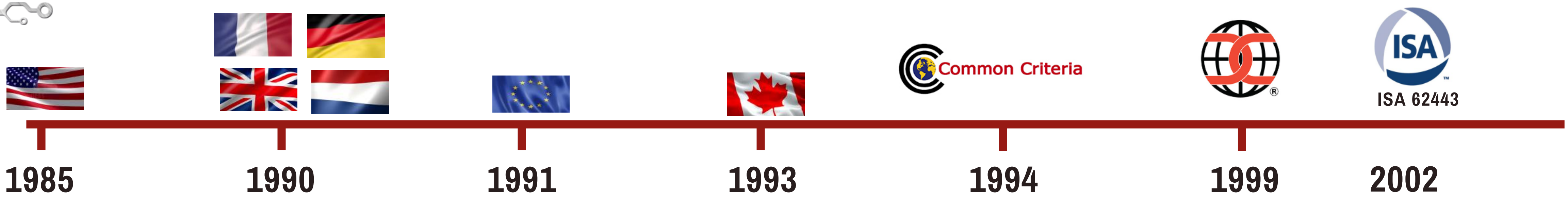
- Actors & Roles within the framework
  - EU Commission, ENISA, NCCA, ECCG, SCCG, AWG

4. Cybersecurity Certification Schemes

- Security Objectives
- Requirements
- Assurance Levels
- Conformity Assessment
- Authorities & Accreditation (NAB, NCCA)
- Evaluation Methodology
- Judicial Remedy & Penalties

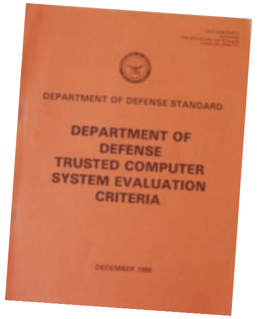
INTRODUCTION TO
ICT PRODUCTS, PROCESSES & SERVICES CERTIFICATION

ICT PRODUCTS CERTIFICATION: HISTORY



- USA: The Orange Book (TCSEC)
- UK: The Green Book (CESG + DTI)
- UK, France, Germany, Netherlands: ITSEC
- Canada: CTCPEC

- Common Criteria
- ISO/IEC 15408


DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

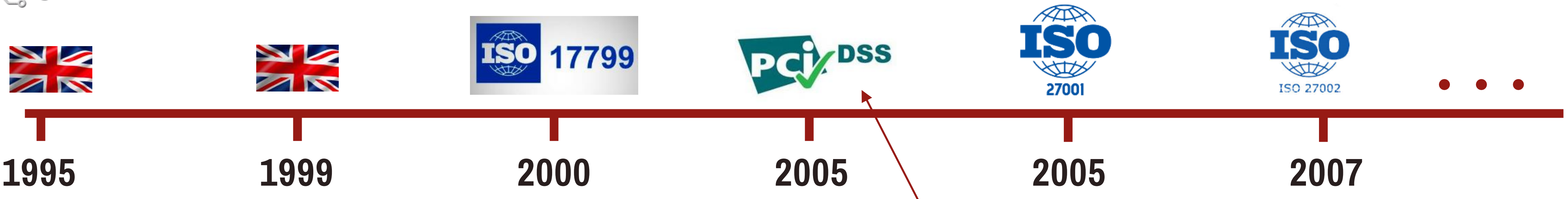
DECEMBER 1985

HM Treasury

THE GREEN BOOK

CENTRAL GOVERNMENT GUIDANCE ON APPRAISAL AND EVALUATION

ICT PROCESS CERTIFICATION: HISTORY



1995 1999 2000 2005 2005 2007

- UK: DTI BSI 7799 (1995)
- UK: DTI BSI 7799 part2 (1999)
- BSI 7799 => ISO 17799 (2000)
- BSI 7799 part2 => ISO 27001 (2005)
- ISO 17799 => ISO 27002 (2007)

Other certifications started popping up

ICT CERTIFICATION: BY DOMAIN

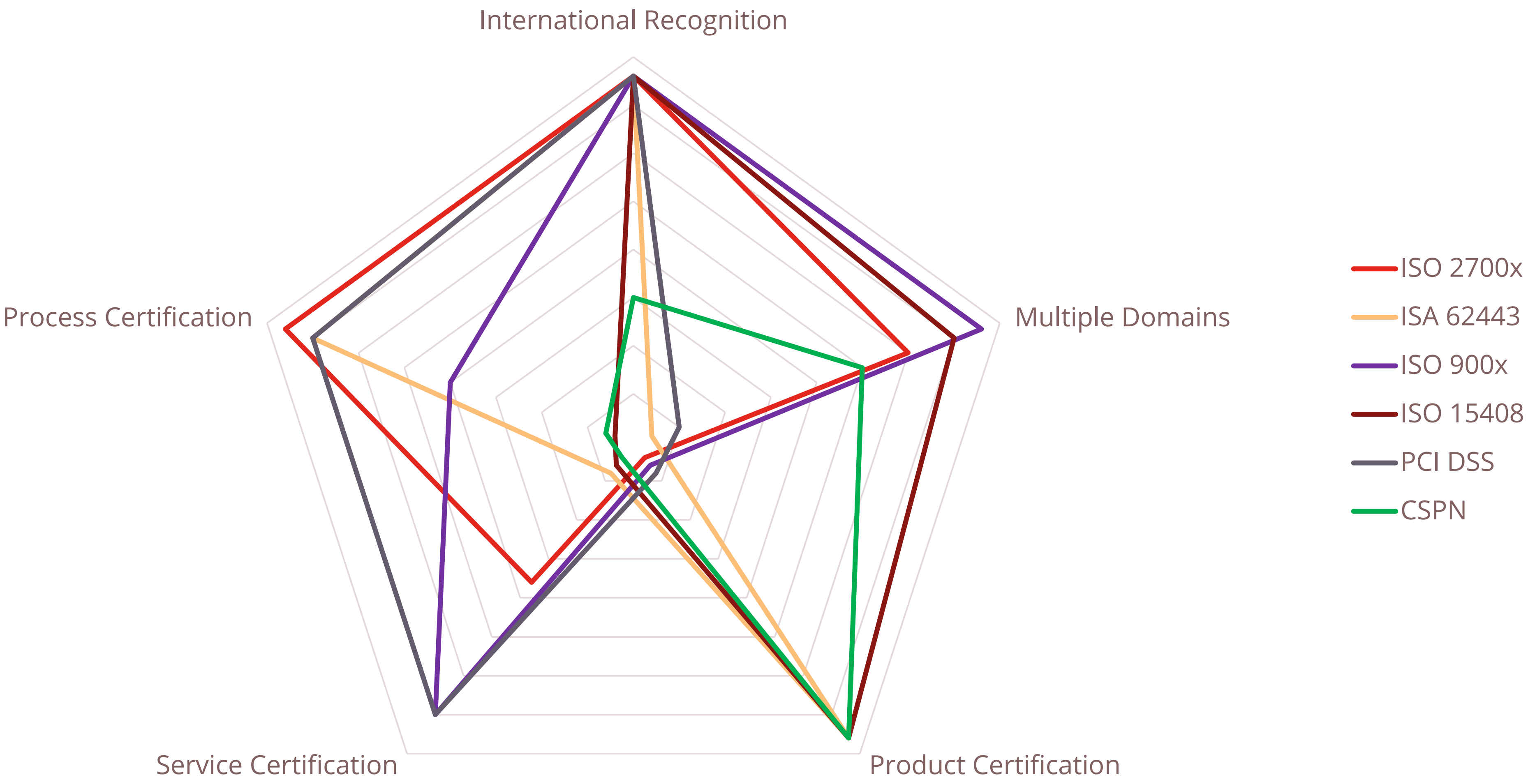
Domain Specific: These are certifications that cover a specific domain.

PCI DSS	Payment Card Industry Data Security
IEC 62443	Industrial Systems Devices & Processes

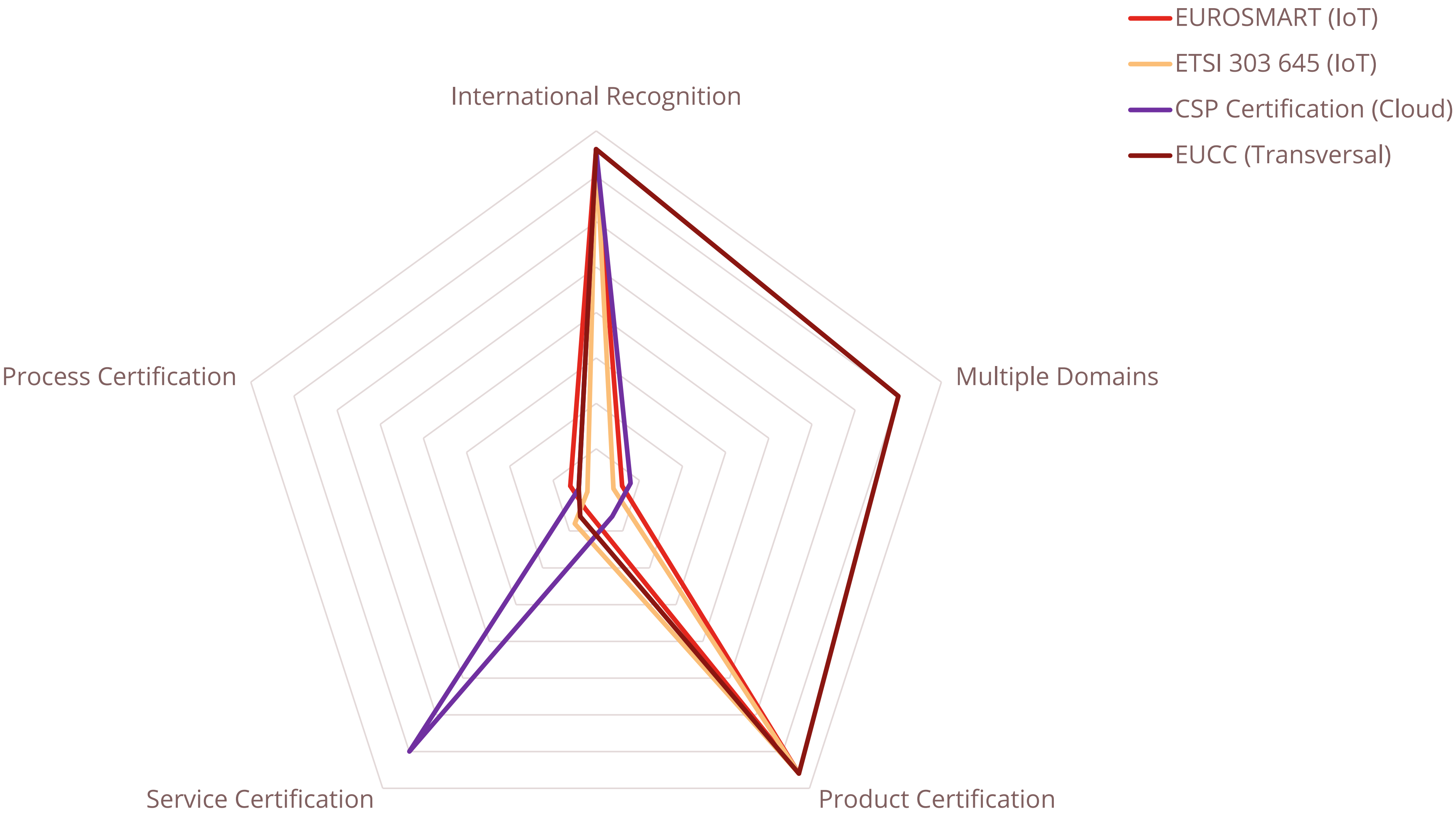
Domain non-specific: These are certifications that are domain agnostic or are applicable to multiple domains.

ISO 2700x	ICT Processes
ISO 15408	ICT Products
CSPN	ICT Products

Scope & Types of ICT Certification



Scope of EU Candidate Certifications



CURRENT STATUS & NEXT STEP FOR CERTIFICATION

ENISA next steps for certifications schemes.

EU CYBERSECURITY ACT
EU CSA

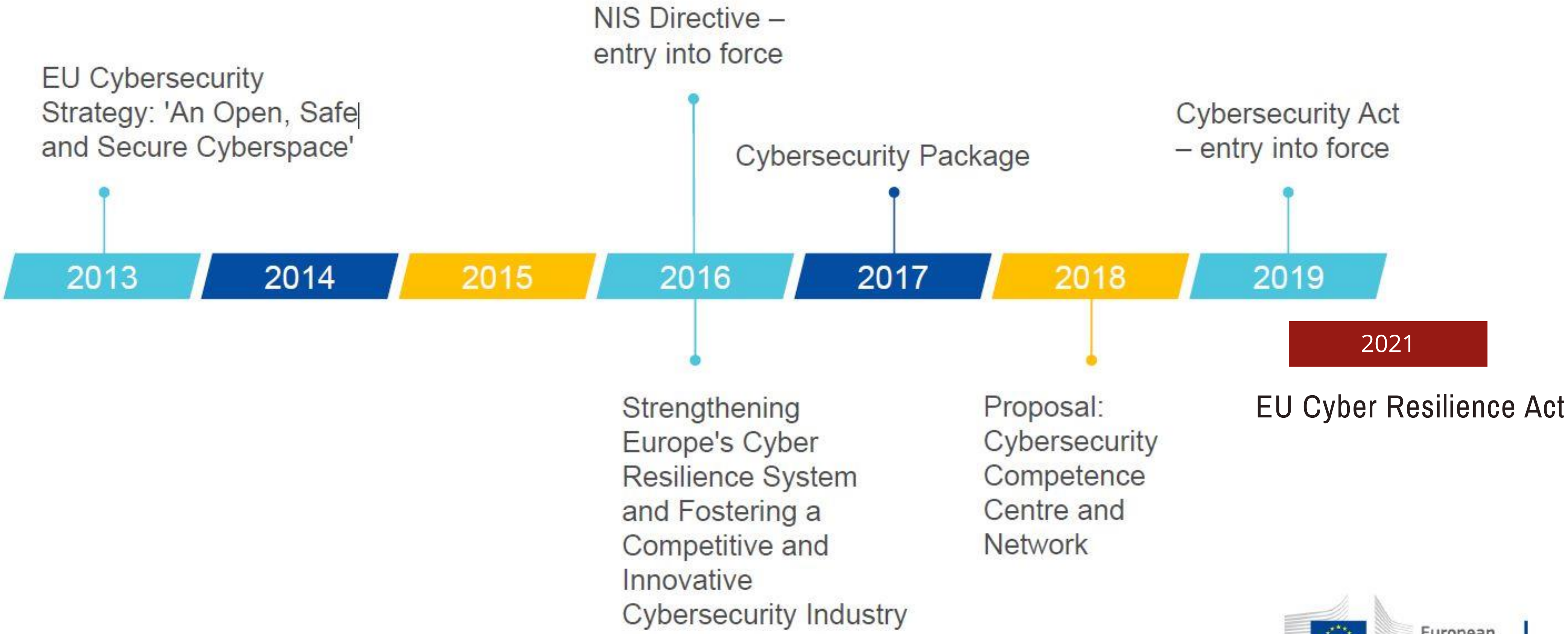
DEFINITION

- Revamps and strengthens the EU Agency for cybersecurity, ENISA (17)

- Establishes an EU-wide cybersecurity certification framework for digital products, services and processes. (48)

- Certification of ICT products, processes and services are recognised across the European Union. (69)

HISTORY



2013

EU Cybersecurity Strategy: 'An Open, Safe and Secure Cyberspace'

2014

2015

2016

NIS Directive – entry into force

Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

2017

Cybersecurity Package

2018

Proposal: Cybersecurity Competence Centre and Network

2019

Cybersecurity Act – entry into force

2021

EU Cyber Resilience Act

QUIZ

- **Mention 1 point of what the CYBER ACT seeks to achieve ?**

- **When was the latest cybersecurity act adopted ?**

- **What is the earliest cybersecurity certification scheme ?**

QUIZ

- **Mention 1 point of what the CYBER ACT seeks to achieve ?**
  - ➢ **Revamps and strengthens the EU Agency for cybersecurity, ENISA (17),**
  - ➢ **Establishes an EU-wide cybersecurity certification framework for digital products, services and processes. (48)**
  - ➢ **Certification of ICT products, processes and services are recognized across the European Union. (69)**

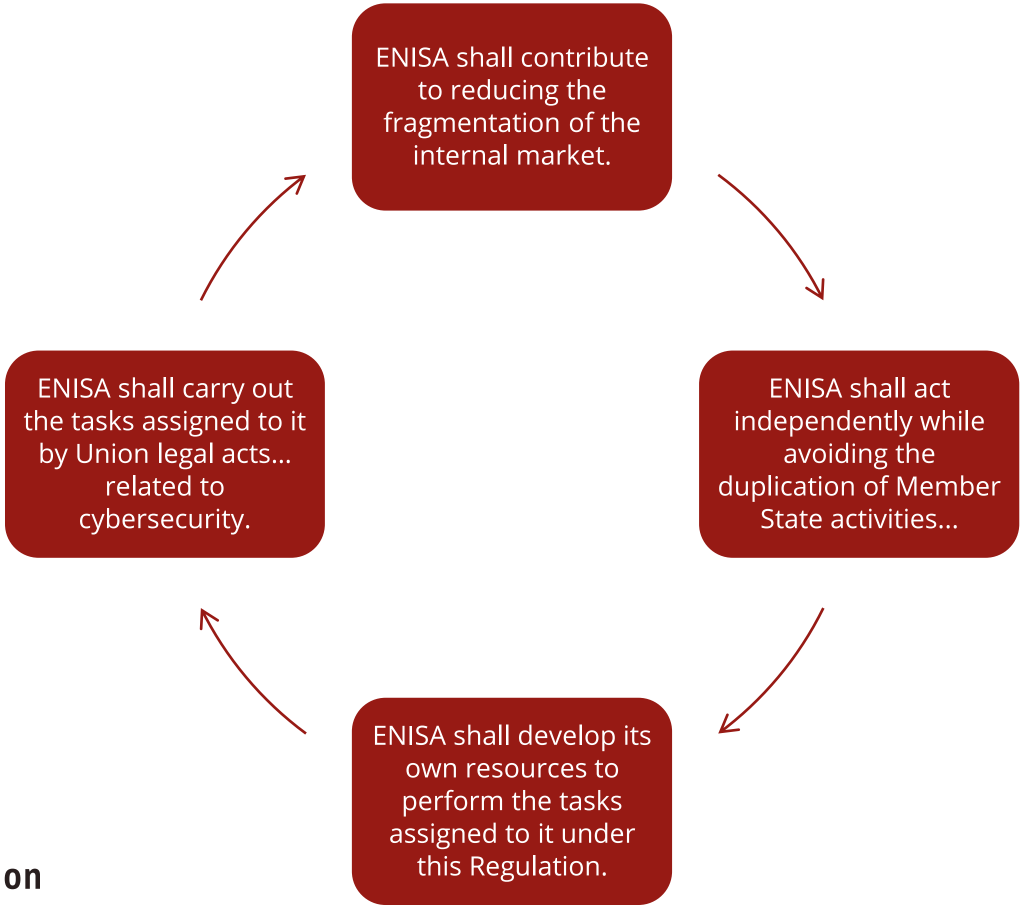
- **When was the latest cybersecurity act adopted ?**
  - ➢ **April 2019**

- **What is the earliest cybersecurity certification ?**
  - ➢ **Orange Book, USA 1985**

EUSA: ENISA MANDATE & TASKS

enisa

European Network and Information Security Agency



ENISA shall contribute to reducing the fragmentation of the internal market.

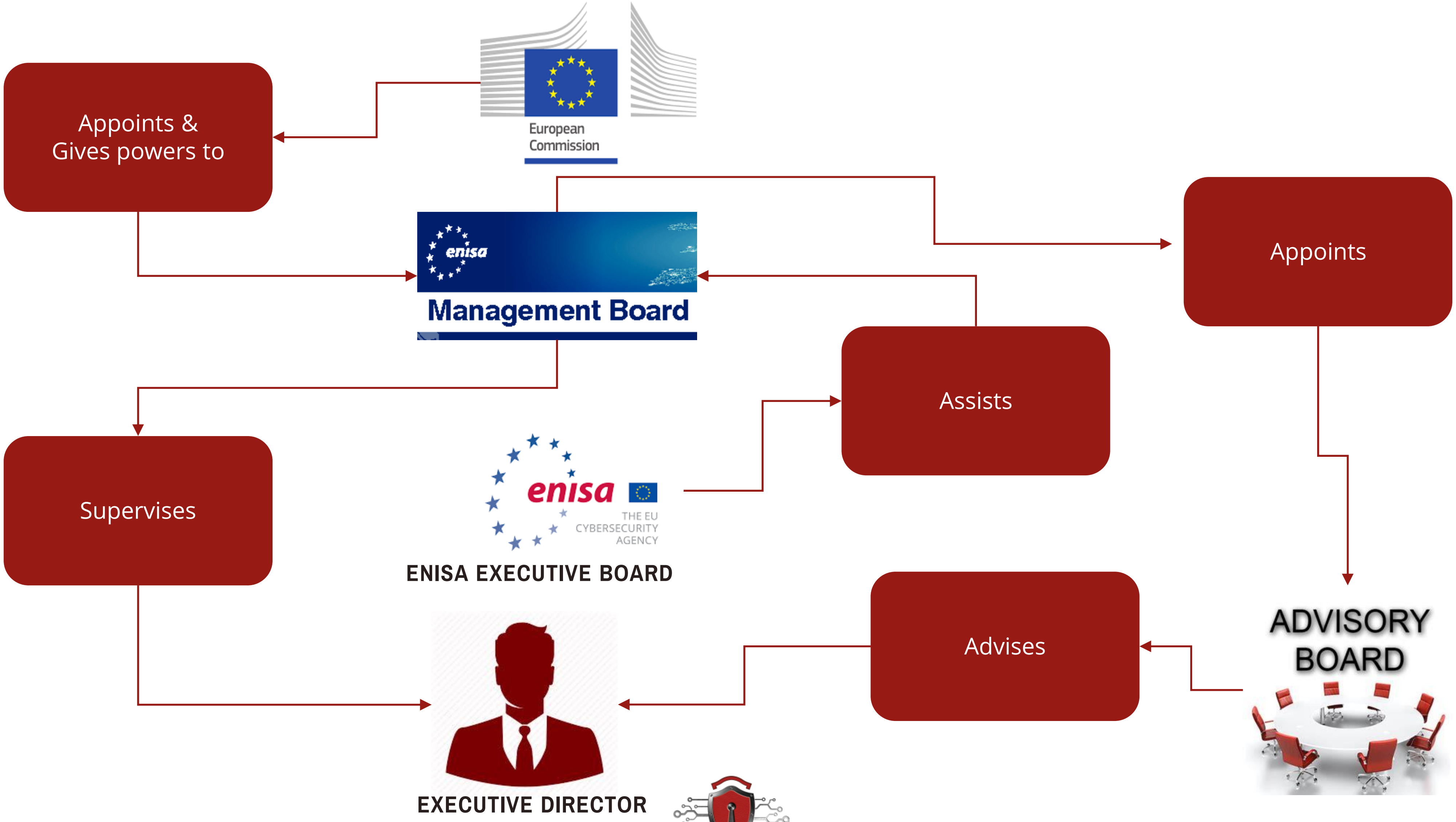
ENISA shall act independently while avoiding the duplication of Member State activities...

ENISA shall develop its own resources to perform the tasks assigned to it under this Regulation.

ENISA shall carry out the tasks assigned to it by Union legal acts... related to cybersecurity.

- Development and implementation of Union law
- Capacity building
- Market cybersecurity certification and standardization
- Raise awareness and enhance cooperation

EUCSA: ENISA GOVERNANCE STRUCTURE



EUCSA: BENEFITS TO STAKEHOLDERS

Vendors

Customers

Regulatory bodies

EUCSA: BENEFITS TO VENDORS

- Demonstrate that their products or services have been attested to fulfil specific requirements
- Provide evidence to the market and to regulators of their commitment to good cybersecurity practices
- Possible re-use of certificates

EUCSA: BENEFITS TO CUSTOMERS

Providing them with the appropriate level of confidence that specific requirements have been fulfilled

Capture and expresses requirements from broad communities of end users

EUCSA: BENEFITS TO REGULATORS

Demonstrate the presumption of conformity with advancements in cybersecurity (European level or Member state level)

QUIZ

- **Who appoints the advisory board ?**
- **What is the role of ENISA executive board ?**
- **Who is responsible for the supervision of ENISA Executive director ?**
- **How does CSA benefit regulators?**

QUIZ

- **Who appoints the advisory board ?**

  - ➢ **Management board appoints the advisory board**

- **What is the role of ENISA executive board ?**

  - ➢ **Executive board (consists 5members drawn from the management board) for a 4-year tenure.**
    - ➢ **Prepare decisions to be adopted by management board**
    - ➢ **Ensure the adequate follow-up to the findings and recommendations stemming from investigations, and the various internal or external audit reports and evaluations**
    - ➢ **Assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters**

- **Who is responsible for the supervision of ENISA Executive director ?**

  - ➢ **Management board supervises the Executive director**

- **How does CSA benefit regulators through the certification?**

  ➢ **Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act**

  ➢ **In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements**

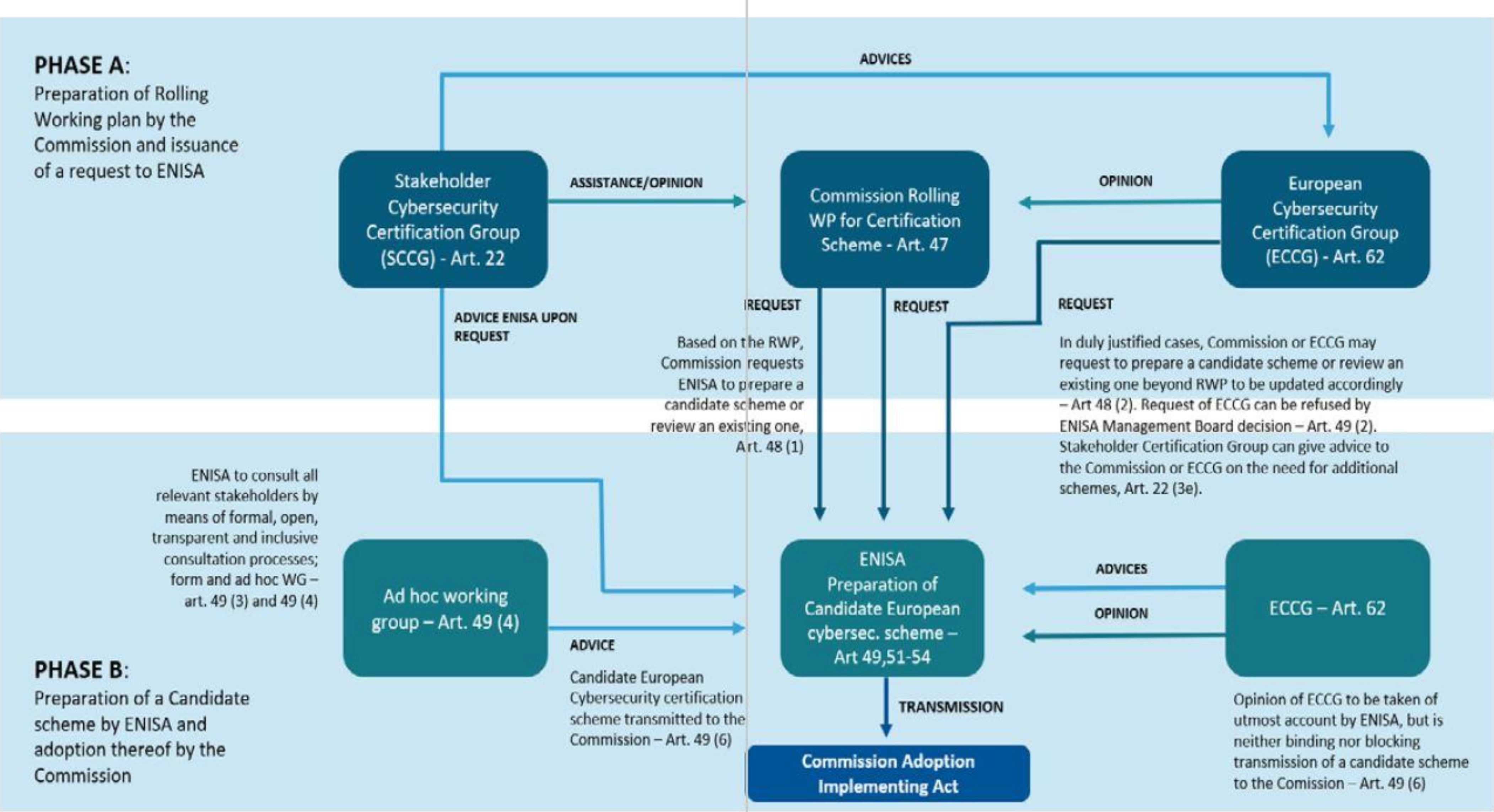
02

EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

This presentation describes each actor and their role as defined within the EU CSA-defined European certification framework.

This presentation does not include their role within a specific scheme (this will be covered in subsequent presentations of iso, EUCC and EUROSMART)

CYBERSECURITY CERTIFICATION FRAMEWORK



PHASE A:
Preparation of Rolling Working plan by the Commission and issuance of a request to ENISA

ADVICES

Stakeholder Cybersecurity Certification Group (SCCG) - Art. 22

ASSISTANCE/OPINION

Commission Rolling WP for Certification Scheme - Art. 47

OPINION

European Cybersecurity Certification Group (ECCG) - Art. 62

ADVICE ENISA UPON REQUEST

REQUEST

Based on the RWP, Commission requests ENISA to prepare a candidate scheme or review an existing one, Art. 48 (1)

REQUEST

REQUEST

In duly justified cases, Commission or ECCG may request to prepare a candidate scheme or review an existing one beyond RWP to be updated accordingly – Art 48 (2). Request of ECCG can be refused by ENISA Management Board decision – Art. 49 (2). Stakeholder Certification Group can give advice to the Commission or ECCG on the need for additional schemes, Art. 22 (3e).

ENISA to consult all relevant stakeholders by means of formal, open, transparent and inclusive consultation processes; form and ad hoc WG – art. 49 (3) and 49 (4)

Ad hoc working group – Art. 49 (4)

ADVICE

Candidate European Cybersecurity certification scheme transmitted to the Commission – Art. 49 (6)

ENISA Preparation of Candidate European cybersec. scheme – Art 49,51-54

ADVICES

OPINION

ECCG – Art. 62

TRANSMISSION

Commission Adoption Implementing Act

Opinion of ECCG to be taken of utmost account by ENISA, but is neither binding nor blocking transmission of a candidate scheme to the Comission – Art. 49 (6)

PHASE B:
Preparation of a Candidate scheme by ENISA and adoption thereof by the Commission

EUCSA: ACTORS AND ROLES

EUROPEAN COMMISSION

ENISA

VARIOUS GROUPS

EUCSA: ACTORS AND ROLES

enisa

Management Board

- Comprises members from each member country
- Supervises the Executive Director
- Ensures ENISA functions in accordance with its mandate.

(Article 15)

EUCSA: ACTORS AND ROLES

European Commission

Article 47

- Publish a Union rolling work programme for European cybersecurity certification
- Request ENISA to prepare a candidate scheme or review an existing scheme

EUCSA: ACTORS AND ROLES

(Article 49)

Prepare a candidate scheme or to review an existing European cybersecurity certification scheme:

- based on the Union rolling work programme.
- which is not included in the Union rolling work programme.

EUCSA: ACTORS AND ROLES

National Cybersecurity Certification Authorities (NCCA)
Article 62.2

- ➡ Each Member State designates one or more national cybersecurity certification authorities in its territory or with mutual agreement, in the territory of another Member State
- ➡ Participate in ECCG (EU Cybersecurity Certification Group)
- ➡ Monitor & supervise activities of CABs & Public bodies functioning as CABs
- ➡ Enforce rules as described in EU certification schemes

EUCSA: ACTORS AND ROLES

EUROPEAN CYBERSECURITY CERTIFICATION GROUP (ECCG)
Article 62

- Comprises national cybersecurity certification authorities from member countries.
- Advise & assist ENISA in EU CSA implementation.
- Advise & assist ENISA in preparing candidate schemes. Article 48
- Facilitate cooperation between national cybersecurity certification authorities
- Facilitate alignment of European cybersecurity certification schemes with internationally recognised standards

EUCSA: ACTORS AND ROLES

STAKEHOLDER CYBERSECURITY CERTIFICATION GROUP (SCCG)
Article 22

- Composed of members selected from amongst recognised experts representing the relevant stakeholders.
- Advice the Commission & ECCG on the need for additional certification schemes.
- Advise ENISA on general and strategic matters relating to the market, cybersecurity certification, and standardisation.
- Advise the Commission on strategic issues regarding the Eu certification framework.
- Assist the commission in the preparation of the Union rolling work programme.

WHAT IS EUCSA ? ACTORS AND ROLES

ADHOC WORKING GROUP (AWG)
Article 20

- Appointed by the Executive Director of ENISA after notifying the management board.
- Tasked with providing to ENISA, specific advice and expertise on a subject matter e.g. a candidate scheme.
- Committee members must declare any conflict of interest

WHAT IS EUCSA ? ACTORS AND ROLES

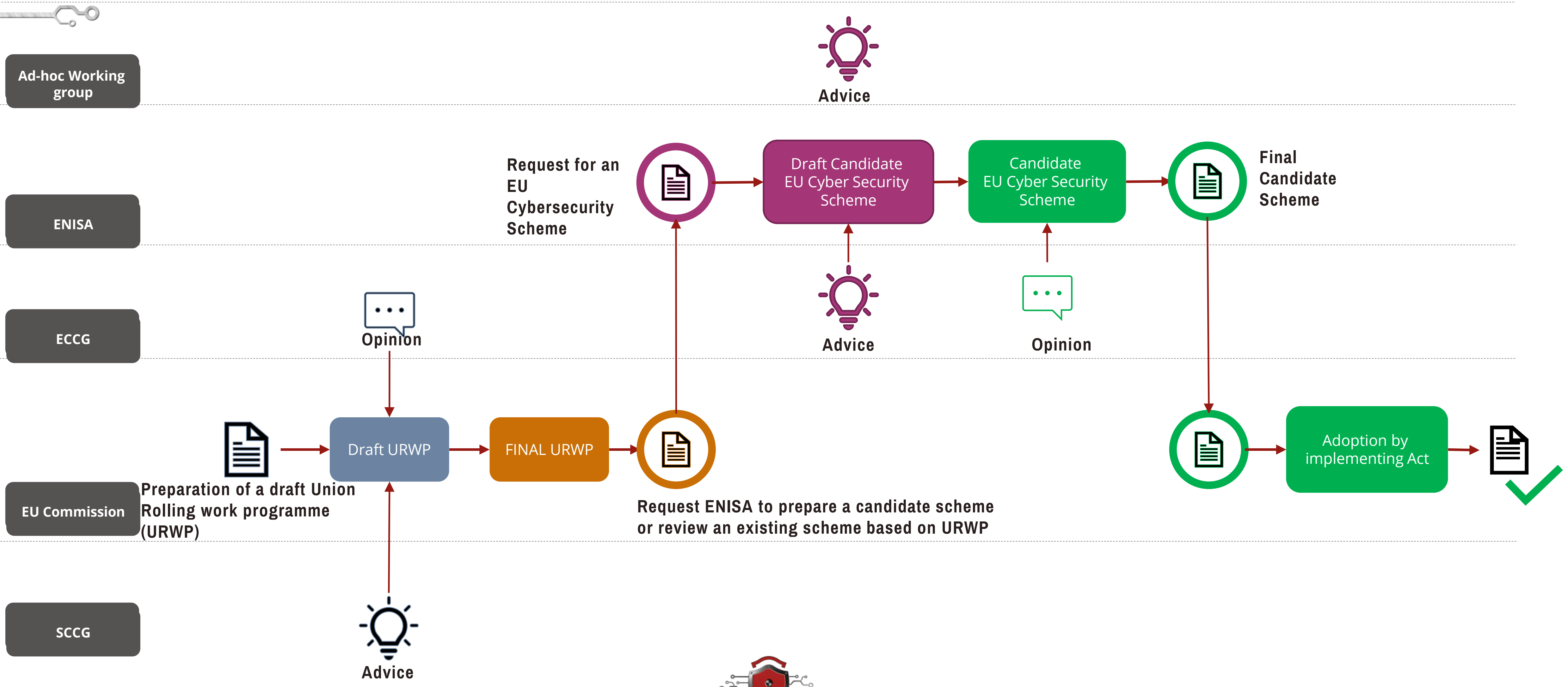
- Transmits Candidate scheme to the Commission after interacting with ECCG, SCCG, Adhoc working Group and other Industry and standardisation bodies

WHAT IS EUCSA ? ACTORS AND ROLES

European Commission

- Take due account of the opinions issued by the ECCG and the Stakeholder Certification Groups.
- Adopts the Candidate scheme for use within the Union

EU CYBERSECURITY CERTIFICATION FRAMEWORK



Ad-hoc Working group
ENISA
ECCG
EU Commission
SCCG
Advice
Request for an EU Cybersecurity Scheme
Draft Candidate EU Cyber Security Scheme
Candidate EU Cyber Security Scheme
Final Candidate Scheme
Advice
Opinion
Opinion
Draft URWP
FINAL URWP
Adoption by implementing Act
Preparation of a draft Union Rolling work programme (URWP)
Request ENISA to prepare a candidate scheme or review an existing scheme based on URWP
Advice

QUIZ

- **List 3 stakeholders & their role(s) within the context of the scheme certification framework ?**

- **What is the role of the NCCA in a Cybersecurity scheme preparation process?**

- **At what stage does ECCG give an opinion on a candidate scheme?**

- **Which comes first within the framework?**

- PREPARATION OF A DRAFT UNION ROLLING WORK PROGRAMME (URWP)
- REQUEST ENISA TO PREPARE A CANDIDATE SCHEME

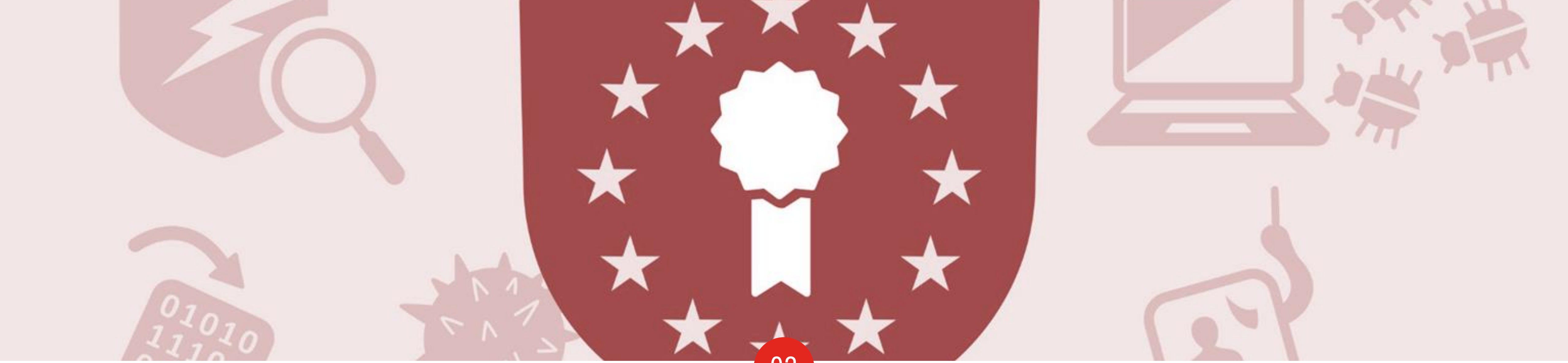
QUIZ

- List 3 stakeholders & their role(s) within the context of the scheme certification framework ?
  - ➢ EU commission, ENISA, SCCG, ECCG, Adhoc working Group, NCCA.
- What is the role of the NCCA in a Cybersecurity scheme preparation process?
  - ➢ They provide input in scheme development via their membership of the ECCG.
- At what stage does ECCG give an opinion on a candidate scheme?
  - ➢ Candidate scheme
- Which comes first within the framework?

- PREPARATION OF A DRAFT UNION ROLLING WORK PROGRAMME (URWP)
- REQUEST ENISA TO PREPARE A CANDIDATE SCHEME

WHAT HAPPENS TO EXISTING NATIONAL SCHEMES ?

- ➡ National schemes whose scope is not covered by a European scheme will remain
- ➡ Member states should not introduce new schemes that covers the same scope as an existing European scheme
- ➡ Existing national certificates that are within scope of an existing European scheme remain valid until they expire



03

CYBERSECURITY CERTIFICATION SCHEMES

EU CERTIFICATION SCHEMES: SECURITY OBJECTIVES

ARTICLE 51

- To protect data during the entire life cycle of the ICT product, ICT service or ICT process.
- Identify and document known dependencies & vulnerabilities.
- Identify and record which data has been accessed & by whom.
- Verify ICT products, services & processes do not contain known vulnerabilities.
- Ensure ICT products, processes & services are secure by default & by design.
- Ensure ICT products, processes & services are securely updated.

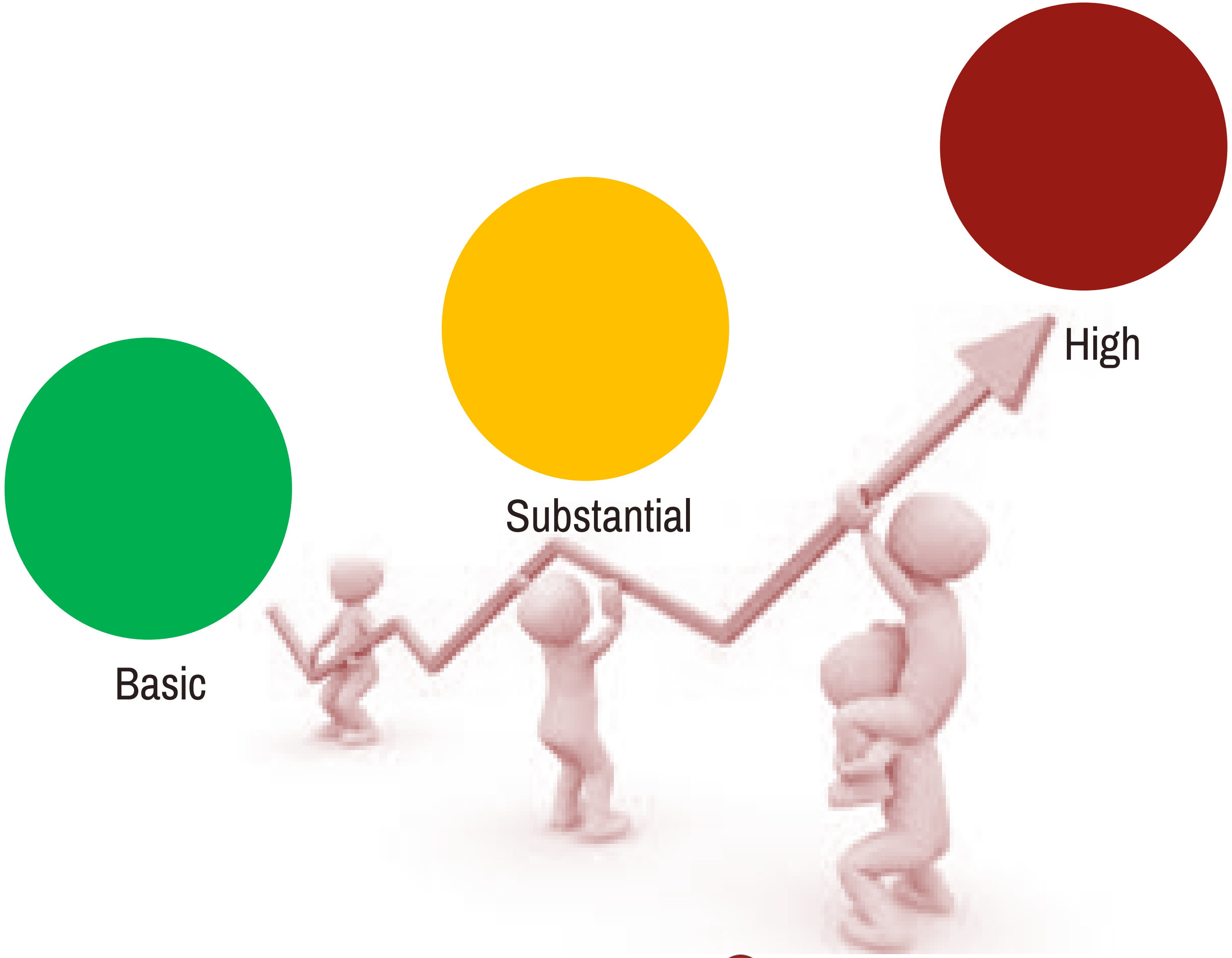
EU CERTIFICATION SCHEMES: REQUIREMENTS

ARTICLE 54

- Describe the scope, purpose, assurance levels and assessment type pertinent to the scheme.
- Make reference to or develop standards, methods and specifications that are consistent with the EU CSA.
- Specify additional requirements for CABs if any.
- Describe a vulnerability detection, reporting and management system.
- Specify rules for demonstrating & maintaining compliance.
- Specify rules for monitoring & sanctioning non-compliance.
- Describe certificates/conformity statements and period their of validity under this scheme.

EU CERTIFICATION SCHEMES: ASSURANCE LEVELS

ARTICLE 52

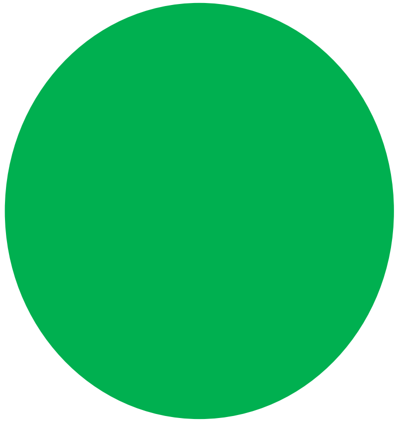


Basic

Substantial

High

EU CERTIFICATION SCHEMES: ASSURANCE LEVELS



Assurance level ‘basic’ provides assurance that the ICT products, services and processes meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of cyber incidents and cyberattacks.

EU CERTIFICATION SCHEMES: ASSURANCE LEVELS

Substantial

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

EU CERTIFICATION SCHEMES: ASSURANCE LEVELS

●

High

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

QUIZ

- Describe the 3 assurance levels presented in EU CSA?
- What happens to a valid certificate issued under a national scheme pre-CSA?
- A certification scheme must not specify extra requirements for a CAB to fulfil, except those specified in the CSA. True or False?

QUIZ

- **Describe the 3 assurance levels presented in EU CSA?**
  - **Basic Substantial, High**
- **What happens to a valid certificate issued under a national scheme pre-CSA?**
  - **It remains valid until its expiry date**
- **A certification scheme must not specify extra requirements for a CAB to fulfil, except those specified in the CSA. True or False?**
  - **False**

EU CERTIFICATION SCHEMES: CONFORMITY ASSESSMENT

Self Assessment

Third party assessment (CABs)

➡ European cybersecurity certification schemes could provide for a conformity assessment to be carried out by:

- conformity self-assessment.
- third party assessments and certifications.
- both self-assessment and 3rd party assessment

EU CERTIFICATION SCHEMES: CONFORMITY ASSESSMENT

Self Assessment

ARTICLE 53

- Issuing conformity statements is voluntary.
- Issuer shall assume responsibility for the compliance of the ICT product, ICT service or ICT process with the requirements set out in the relevant scheme.
- Conformity statements shall be recognised in all member states.
- The conformity statement must be made available to the NCCA and ENISA.
- Self assessments are acceptable for Assurance Level “BASIC” alone.

EU CERTIFICATION SCHEMES: CONFORMITY ASSESSMENT

Third party assessment

- 3rd party assessments (Basic & Substantial) are handled by Conformance Assessment Bodies (CABs)
- CABs are accredited and regulated by National Accreditation Bodies, (NABs) according to the requirements set in the EU CSA. Where a scheme sets additional or specific requirements, only CABs that meet those requirement are authorized to function in such a scheme.
- A scheme may require that certificates are issued only by a public body. This body shall be the NCCA or a public body that is accredited as a CAB. If the assessment is done by the NCCA, the NCCA shall also be accredited as a CAB.
- Certificate for Assurance level of "High" under an EU Cybersecurity Certification scheme can only be issued by an NCCA or a CAB specifically delegated by the NCCA.

EU CERTIFICATION SCHEMES: BECOMING A CAB

Third party assessment
ANNEX

- Shall be a legal entity under a national law
- Shall be independent & avoid conflict of interests.
- Shall demonstrate professional integrity.
- Shall be technically capable, covering all categories of evaluations which it undertakes.
- Shall possess the means & tools necessary to perform evaluations.
- Remunerations shall not depend on number of conformity assessments carried out.
- Shall take a liability insurance.
- Shall be compliant to relevant standards for accreditation of a CAB.

CERTIFICATION SCHEME ? AUTHORITIES

National Cybersecurity Certification Authorities (NCCA)

Article 58

- ➡ Monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes in its respective territory in relation to the EU statement of conformity
- ➡ Monitor relevant developments in cybersecurity certification field.
- ➡ Handle complaints in relation to CAB-issued or NCCA-issued certificates.
- ➡ Share information regarding non-compliance of products processes & services with other NCCAs .
- ➡ NCCA that issues certificates must be accredited as a CAB.
- ➡ Assist NABs in monitoring & supervision of CABs.
- ➡ Issuing certificates, particularly for the “High” assurance level.

CERTIFICATION SCHEME ? ACCREDITATION

National Accreditation Body (NAB)
Article 60

- National accreditation body (NAB) is the sole body in a Member State that performs accreditation with authority derived from the State
- Restrict, suspend or withdraw CABs accreditation due to non-compliance to CSA or a Certification Scheme.
- Accrediting CABs (MAX 5yrs validity).

QUALITY CONTROL APPROVED

CERTIFICATION SCHEME: EVALUATION METHODOLOGY

“BASIC” assurance level

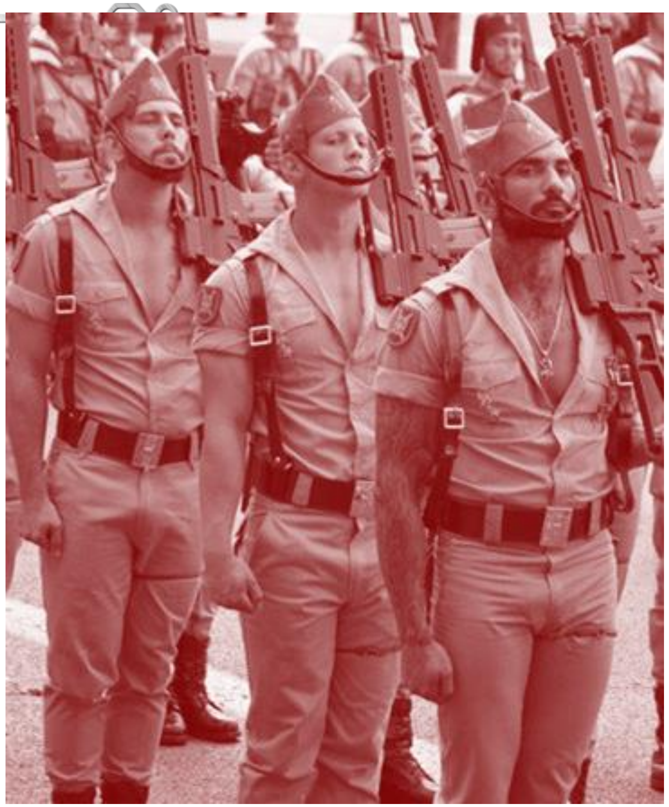
- CABs should at least include a review of the technical documentation of the ICT product, ICT service or ICT process
- ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review by CABs

EU CERTIFICATION SCHEMES: EVALUATION METHODOLOGY

“SUBSTANTIAL” assurance level

➡ In addition to “BASIC”, CABs should verify compliance of the security functions of the ICT product, ICT service or ICT process with its technical documentation.

CERTIFICATION SCHEME: EVALUATION METHODOLOGY



“High” assurance level

- In addition to “SUBSTANTIAL”, CABs should test resistance of the security functions of the ICT product, ICT service or ICT process to cyber attackers who have significant skills and resources.

QUIZ

- For what assurance levels are self assessments applicable?
- Name one example where issuing conformity assessments are compulsory.
- Who is responsible for issuing certificates for “High” assurance level?
- What is the role of NAB ?
- “Substantial” level compliance includes requirements from “Basic”. True or False?

QUIZ

- For what assurance levels are self assessments applicable?

  ➢ Self assessments are allowed for Only Basic.

- Name one example where issuing conformity assessments are compulsory.

  ➢ There is no time where conformity statements are compulsory.

- Who is responsible for issuing certificates for “High” assurance level?

  ➢ NCCA except in exceptions where a CAB is authorized to issue.

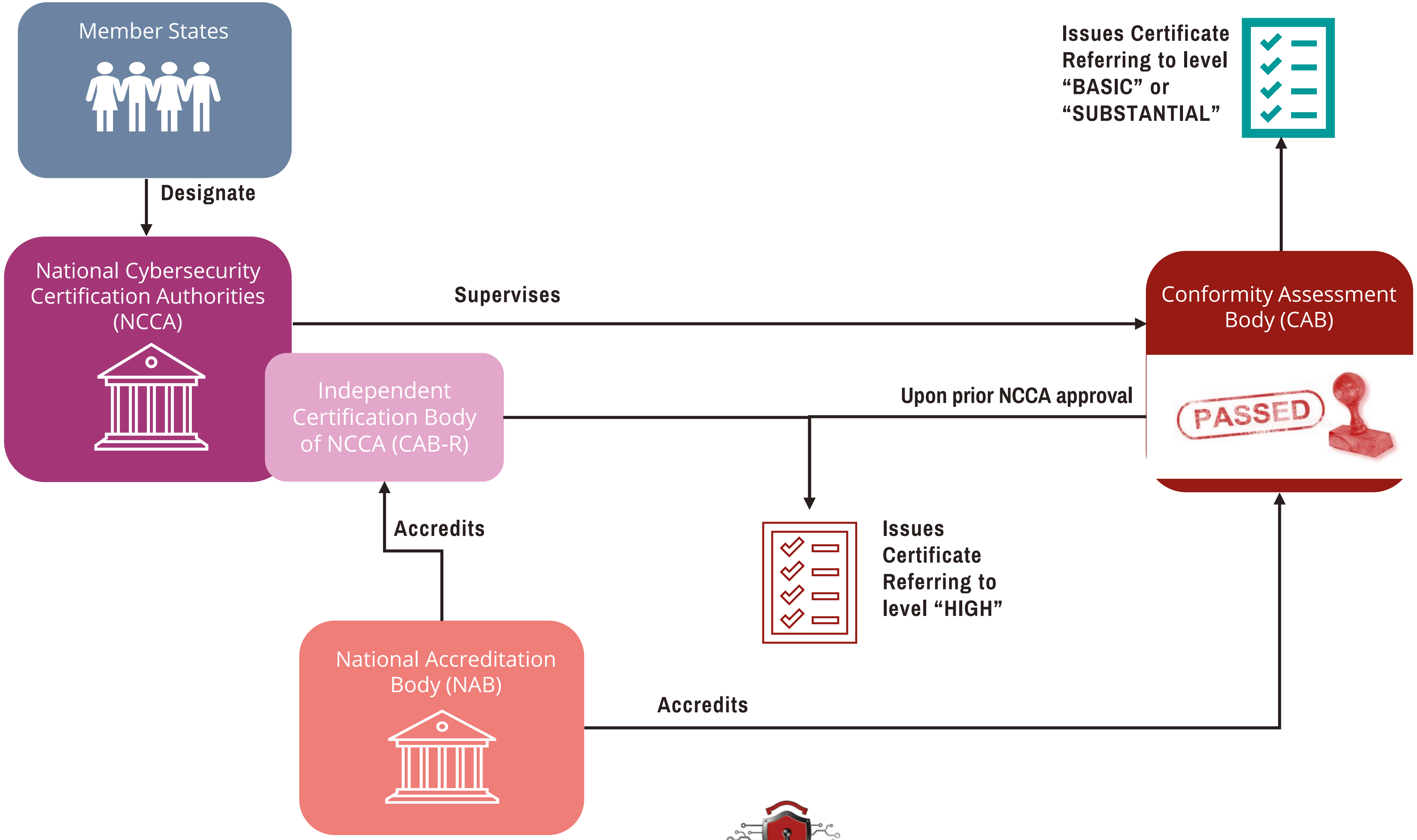
- What is the role of NAB ?

  ➢ NAB is responsible for accreditation. (Issue, Restrict, Suspend, or withdraw a CAB’s accreditation).

- “Substantial” level compliance includes requirements from “Basic”. True or False?

  ➢ True, “substantial” assurance level also includes requirements from “basic”.

EU SCHEMES: CERTIFICATION FRAMEWORK



Member States

Designate

National Cybersecurity Certification Authorities (NCCA)

Independent Certification Body of NCCA (CAB-R)

Supervises

Upon prior NCCA approval

Conformity Assessment Body (CAB)

Issues Certificate Referring to level “BASIC” or “SUBSTANTIAL”

Accredits

Issues Certificate Referring to level “HIGH”

National Accreditation Body (NAB)

Accredits

EU CERTIFICATION SCHEMES: JUDICIAL REMEDY

- Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a certificate issued by a CAB for assurance level “High” in accordance with Article 56(6), the complaint Is lodged with the relevant national cybersecurity certification authority.
- Natural and legal persons shall have the right to an effective judicial remedy regarding:
  - decisions taken by the authority or body referred to above, on the improper issuing, failure to issue or recognition of a certificate held by those natural and legal persons;
  - a failure to act on a complaint lodged with the authority or body referred to above
- Proceedings for a judicial remedy shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.

EU CERTIFICATION SCHEMES: PENALTIES

- Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them. The NCCA has this power

CONTACT

Red Alert Labs

3 rue Parmentier| 94140 Alfortville

✉ *contact@redalertlabs.com*

☎ +33 9 53 55 54 11

www.redalertlabs.com

RED ALERT LABS
IoT Security