EUCC & CRA & AI & NIS2 & Chips….

Miguel Bañón
November 14, 2022

Table of Contents

Abstract

The EU legislative initiatives have led the global market in the past for market relevant aspects dealing with privacy and data protection, and recent and coming initiatives are shaping the EU market in aspects dealing with cybersecurity requirements for products, services and processes, where compliance is to be demonstrated by certification based on standards.

On one side, the Cybersecurity Act sets the framework to define EU-wide certification schemes, and there are three such schemes being currently developed by ENISA, the EU Agency for Cybersecurity, EUCC, EU5G and EUCS. On the other side, the NIS2 proposal sets the hook for national strategies that are to secure critical infrastructures to define requirements for the supply chain, and use such schemes to prove compliance.

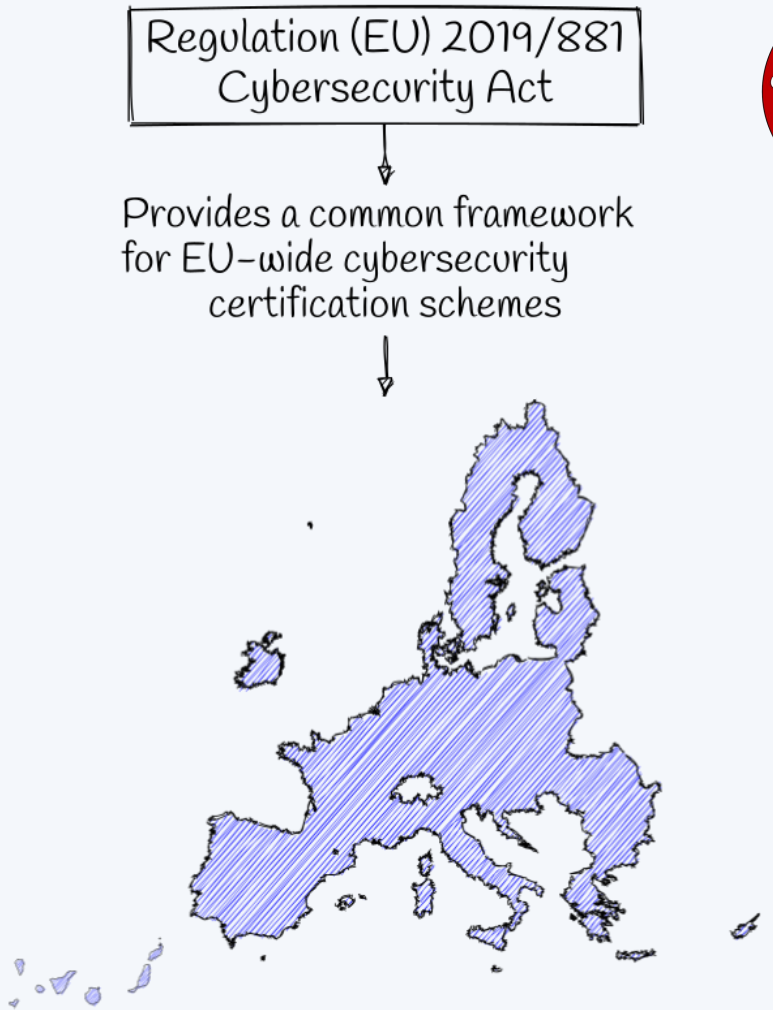
Other initiatives, like the recently announced EU Cyber Resilience Act, will bring a similar approach to the full EU market depicting a final landscape where the EUCC will play a fundamental role.

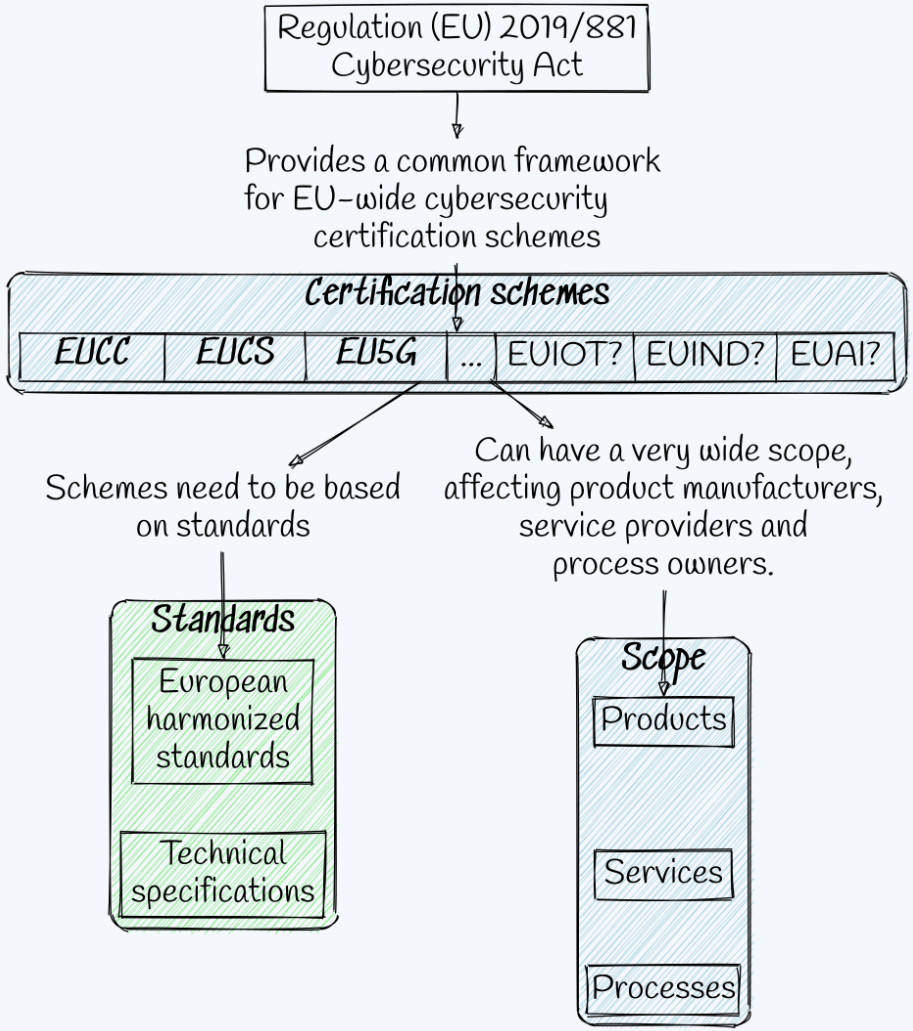
REFERENCES: EU LEGISLATION

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
- Cybersecurity Certification: Candidate EUCC Scheme V1.1.1
- The NIS2 Directive: A high common level of cybersecurity in the EU
- Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence
- Proposal for a regulation on cybersecurity requirements for products with digital elements
- Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem

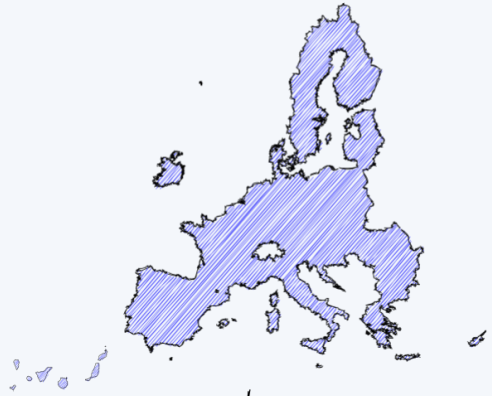
REGULATION (EU) 2019/881, CYBERSECURITY ACT

The CSA is a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.





The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.



New regulations

NIS2	Cyber resilience	AI	Chips	...

New regulations are to request compliance to cybersecurity requirements

Compliance to be demonstrated by applying harmonized standards

Compliance may be required to be demonstrated by a CSA scheme certificate

Harmonized Standards

CEN CENELEC ETSI

Certification schemes

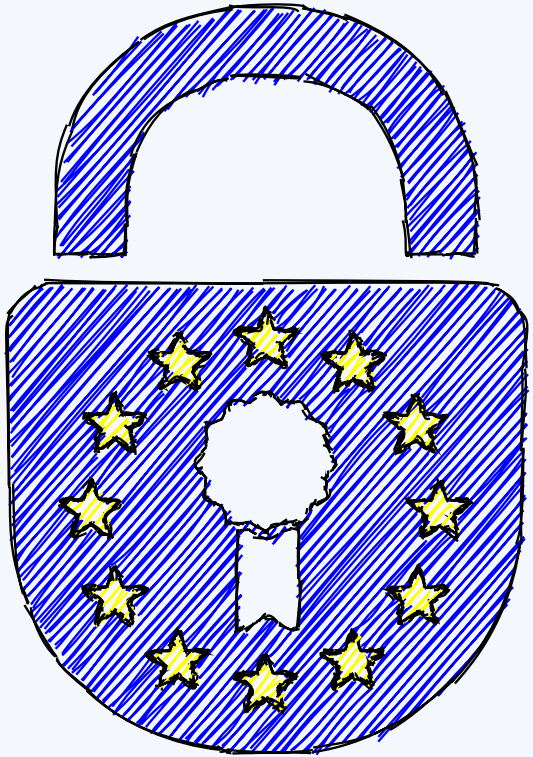
EUCC	EUCS	EU5G	...	EUIOT?	EUIND?	EUAI?

Schemes may be horizontal, like the EUCC, or serve a particular vertical market need.

They will be generally voluntary, and can be conceived as a service. Other regulation may impose cybersecurity requirements to products, services or processes, and can rely on such schemes for the compliance mechanism.

THE EUCC

What is the new EUCC?



Technically, a Common Criteria certification scheme

Legally, the first European certification scheme based on the Cybersecurity Act (CSA).

(Warning: The publicly available scheme proposal will differ from the final implementing act.)

Technicalities

- The EUCC will be irrespectively be based on the Common Criteria and ISO/IEC 15408 standards.

(These are going to be running in parallel for the foreseeable future)

Technicalities

- A product can be certified according to the EUCC if the corresponding security target includes:
  - ALC_FLR - Flaw remediation procedures
  - AVA_VAN - Vulnerability analysis

Those are very simple content requirements.

Technicalities

The EUCC inherits the SOG-IS technical domains and related supporting documents for high assurance level:

- Smartcards and Similar Devices
- Hardware Devices with Security Boxes

Legalities

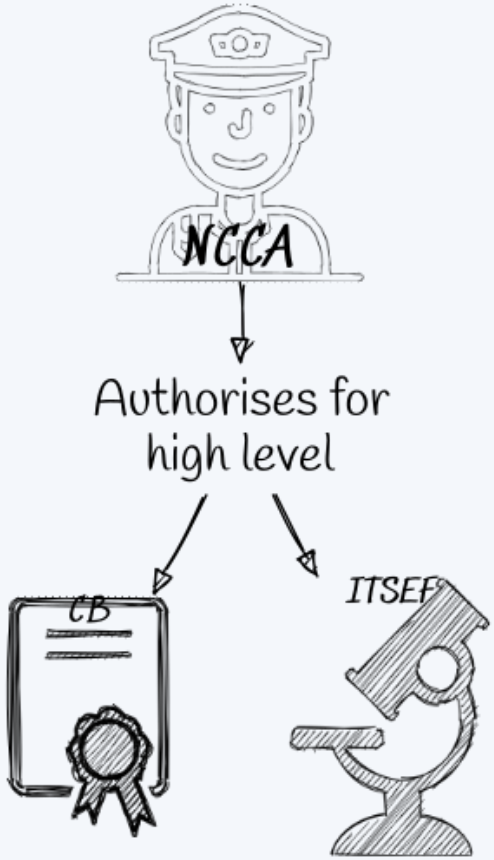
- Certification in CSA is voluntary. Two policy-driven strategies may have a relevant impact in the EUCC certification demand:
  - Coordination in EU public procurement (14% EU GDP, 60% ICT)
  - Further EU regulations and certification schemes

Legalities

Labs need to be accredited ISO/IEC 17025.

Conformity Assessment Bodies (CAB = Certification Body) need to be accredited ISO/IEC 17065.

Both labs and CABs need to be authorized for high assurance level by the local National Cybersecurity Certification Authority.



Legalities

- Existing governmental SOG-IS certification bodies will not operate at substantial assurance level, only at high assurance level.
- Certification at substantial assurance level will only be possible with private CABs.

This opens the capability to certify products to the scale and growth allowed by the private sector. The scenario changes radically.

Legalities

A faster (than SOG-IS) certificate maintenance process is available, provided that the vendor implements a given patch-management policy and procedures.

This is experimental, and very promising.

Legalities

"Rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme."

These will be ultimately country-specific, as developed by each adopting member when approving the National Cybersecurity Certification Authority and related national legislation.

Legalities

"Rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with."

This is new and very hard to comply with. Based on ISO standards, ISO/IEC 29147 and ISO/IEC 30111. Timeline of vulnerability handling and disclosure is very strict.

The CRA also introduces strong requirements for vulnerability handling and disclosure, hopefully more or less in line with the EUCC.

Legalities

"Conditions for the mutual recognition of certification schemes with third countries."

Still under discussion with CCRA, see the CCDB responses from last week.

Timeline

The EUCC implementing act is still pending.

An initial period may be defined to allow all countries be equally ready to start operating in EUCC mode.

After two years of entry into force, national SOG-IS schemes have to cease operation.

Transition to EUCC

- Technically speaking, not much to do from current EAL-based certification projects (check ALC_FLR and AVA_VAN content).
- To comply with the CSA elements and obligations of the scheme, vulnerability handling and disclosure policies and procedures need to be reviewed.
- To take advantage of the faster maintenance route, the patch management policies and procedures need to be reviewed.

Transition to EUCC

SOG-IS certificates can be transformed into EUCC certificates. This can be possible if the original lab becomes an EUCC CAB. The compliance with the CSA legal aspects will focus the effort in this transformation.

NIS2

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Article 1

1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.

2. To that end, this Directive:

(a) lays down obligations on Member States to **adopt national cybersecurity strategies**, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);

Article 5 National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:

(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;

Article 18 *Cybersecurity risk management measures*

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

2. The measures referred to in paragraph 1 shall include at least the following:

(d) supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;

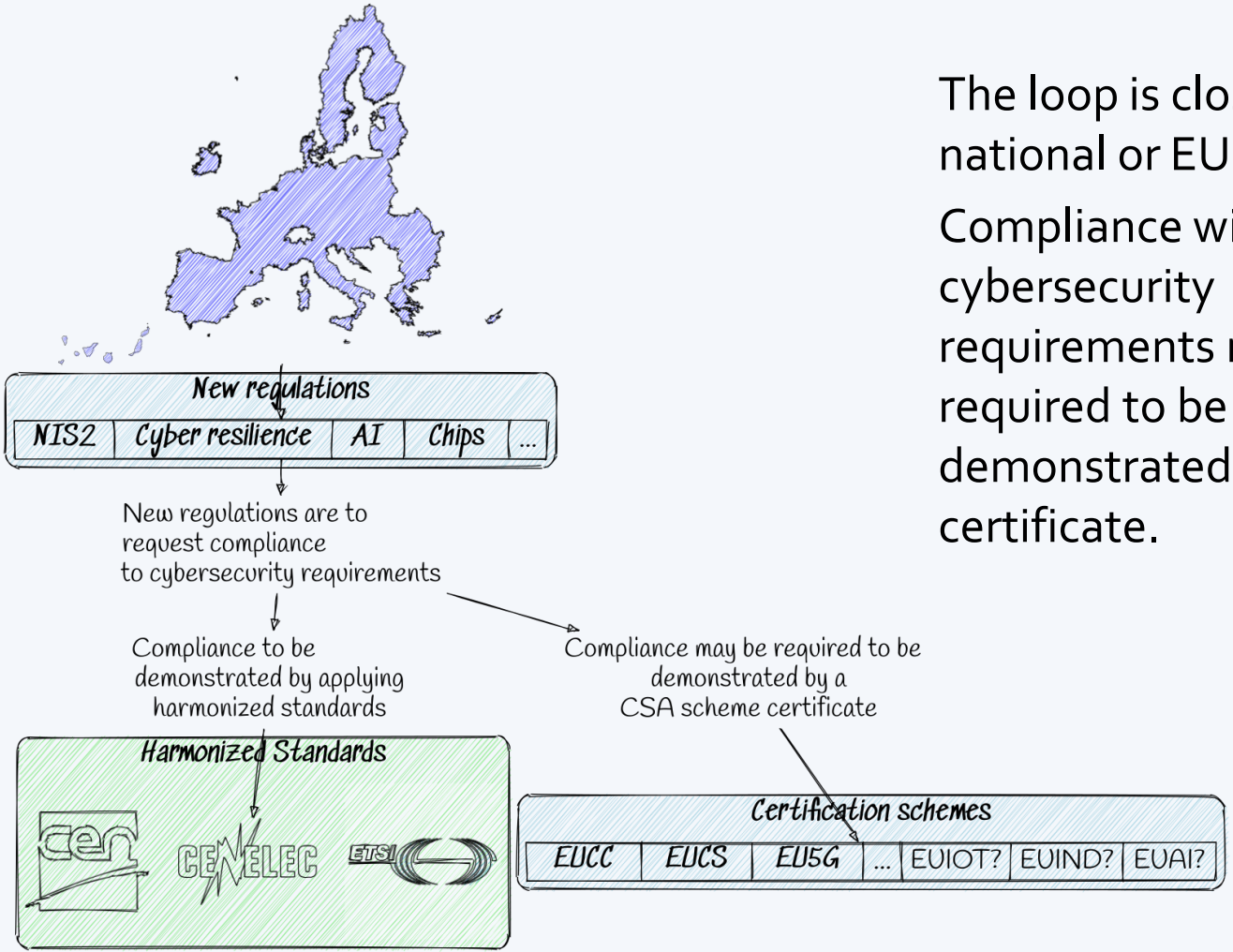
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(g) the use of cryptography and encryption.

Article 21 ***Use of European cybersecurity certification schemes***

1. In order to demonstrate compliance with certain requirements of Article 18, **Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.**

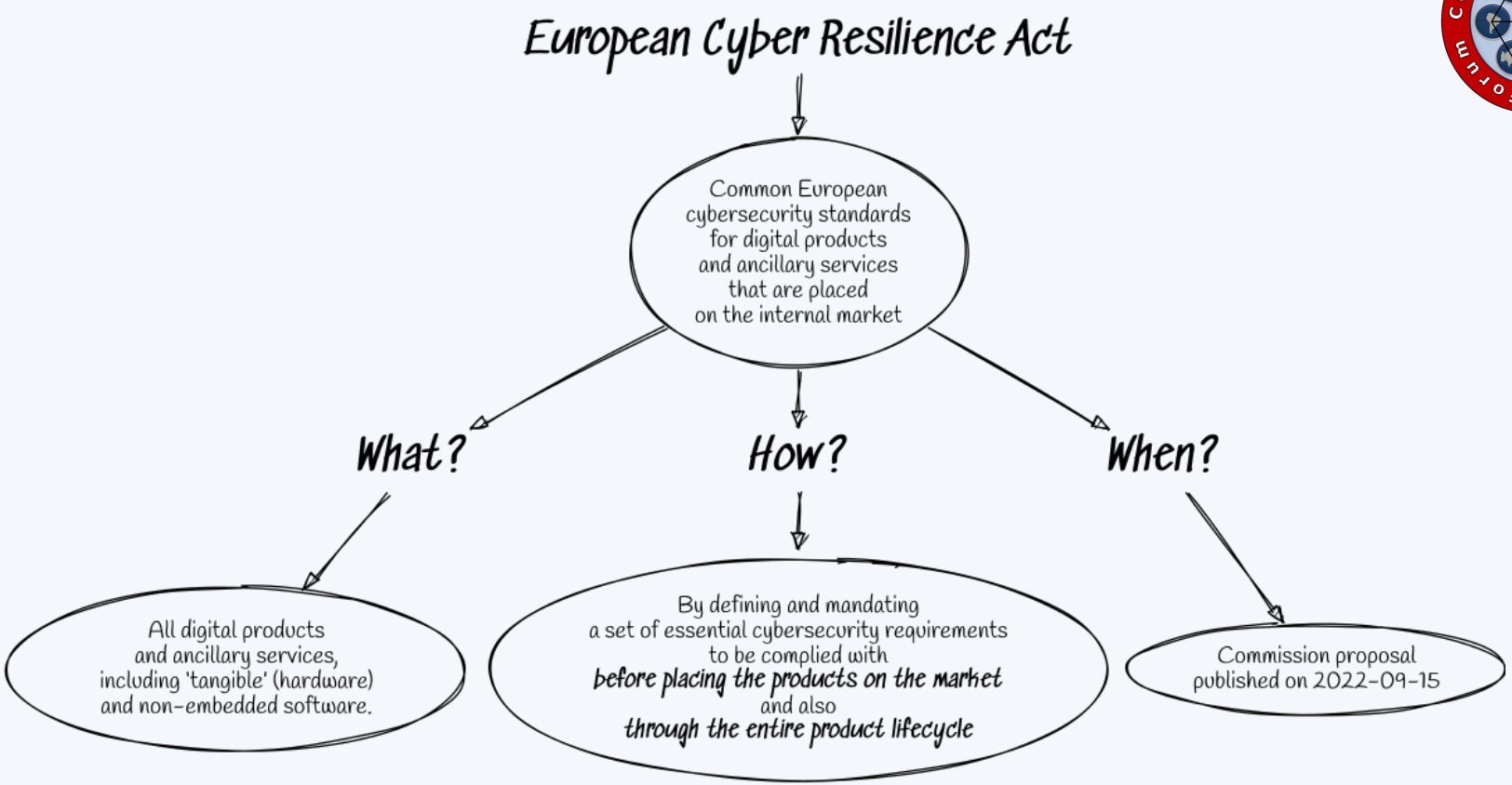
2. The **Commission** shall be empowered to adopt delegated acts specifying which categories of essential entities **shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1**.



The loop is closed, at national or EU-wide level.

Compliance with cybersecurity requirements may be required to be demonstrated with a CSA certificate.

EUROPEAN CYBER RESILIENCE ACT


European Cyber Resilience Act
Common European cybersecurity standards for digital products and ancillary services that are placed on the internal market
What?
How?
When?
All digital products and ancillary services, including 'tangible' (hardware) and non-embedded software.
By defining and mandating a set of essential cybersecurity requirements to be complied with
before placing the products on the market
and also
through the entire product lifecycle
Commission proposal published on 2022-09-15

This Regulation lays down:

(a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;

(b) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;

(c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;

(d) rules on market surveillance and enforcement of the above-mentioned rules and requirements.

This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

(Some exceptions apply)

(High risk AI also in scope)

Essential cybersecurity requirements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

(g) minimise their own negative impact on the availability of services provided by other devices or networks;

(h) be designed, developed and produced to limit attack surfaces, including external interfaces;

(i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;

(k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.

Critical products, class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;

13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;
16. Operating systems not covered by class II;
17. Firewalls, intrusion detection and/or prevention systems not covered by class II;
18. Routers, modems intended for the connection to the internet, and switches, not covered by class II;
19. Microprocessors not covered by class II;
20. Microcontrollers;
21. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
22. Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
23. Industrial Internet of Things not covered by class II.

Critical products, class II

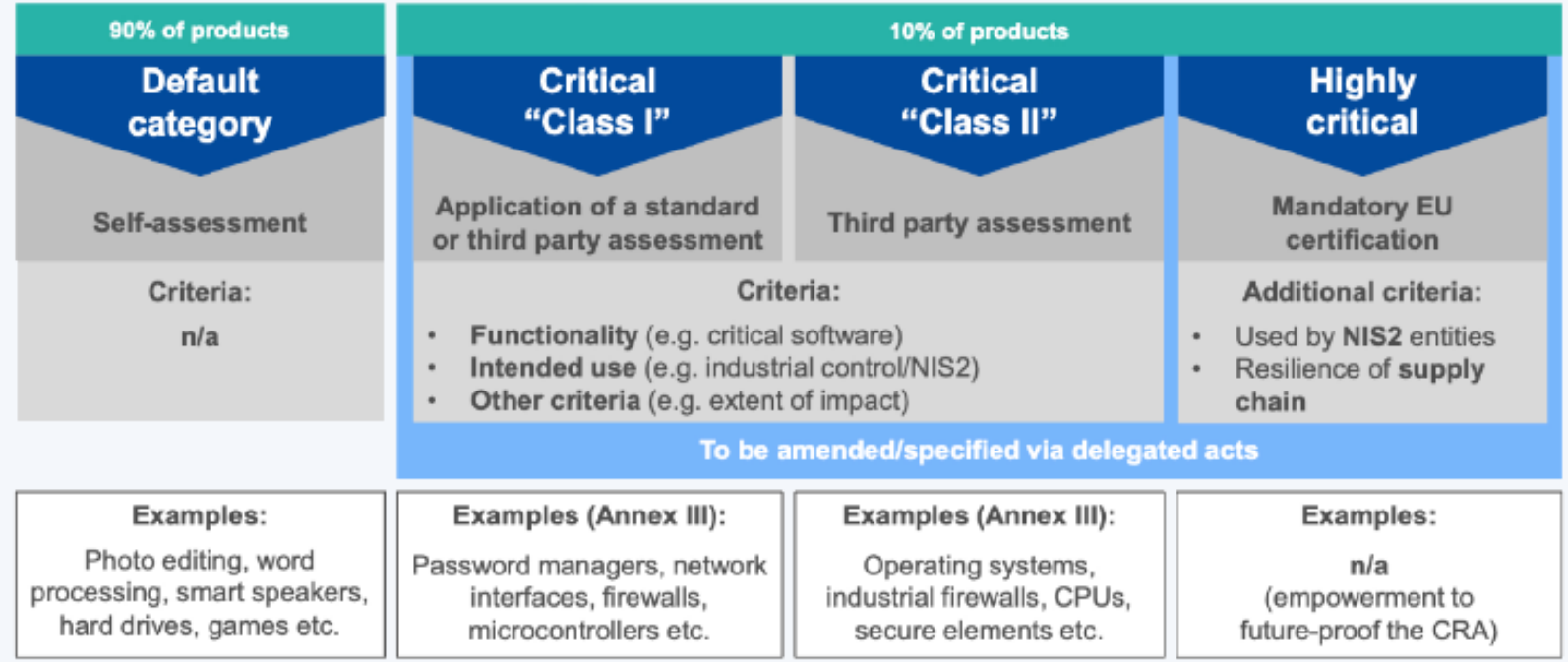
1. Operating systems for servers, desktops, and mobile devices;
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Public key infrastructure and digital certificate issuers;
4. Firewalls, intrusion detection and/or prevention systems intended for industrial use;
5. General purpose microprocessors;
6. Microprocessors intended for integration in programmable logic controllers and secure elements;
7. Routers, modems intended for the connection to the internet, and switches, intended for industrial use;
8. Secure elements;
9. Hardware Security Modules (HSMs);
10. Secure cryptoprocessors;
11. Smartcards, smartcard readers and tokens;
12. Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);
13. Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];
14. Robot sensing and actuator components and robot controllers;
15. Smart meters.

Presumption of conformity, Article 18

4. The Commission is empowered, by means of implementing acts, to specify the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I.

Furthermore, where applicable, the Commission shall specify if a cybersecurity certificate issued under such schemes eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 24(2)(a), (b), (3)(a) and (b).

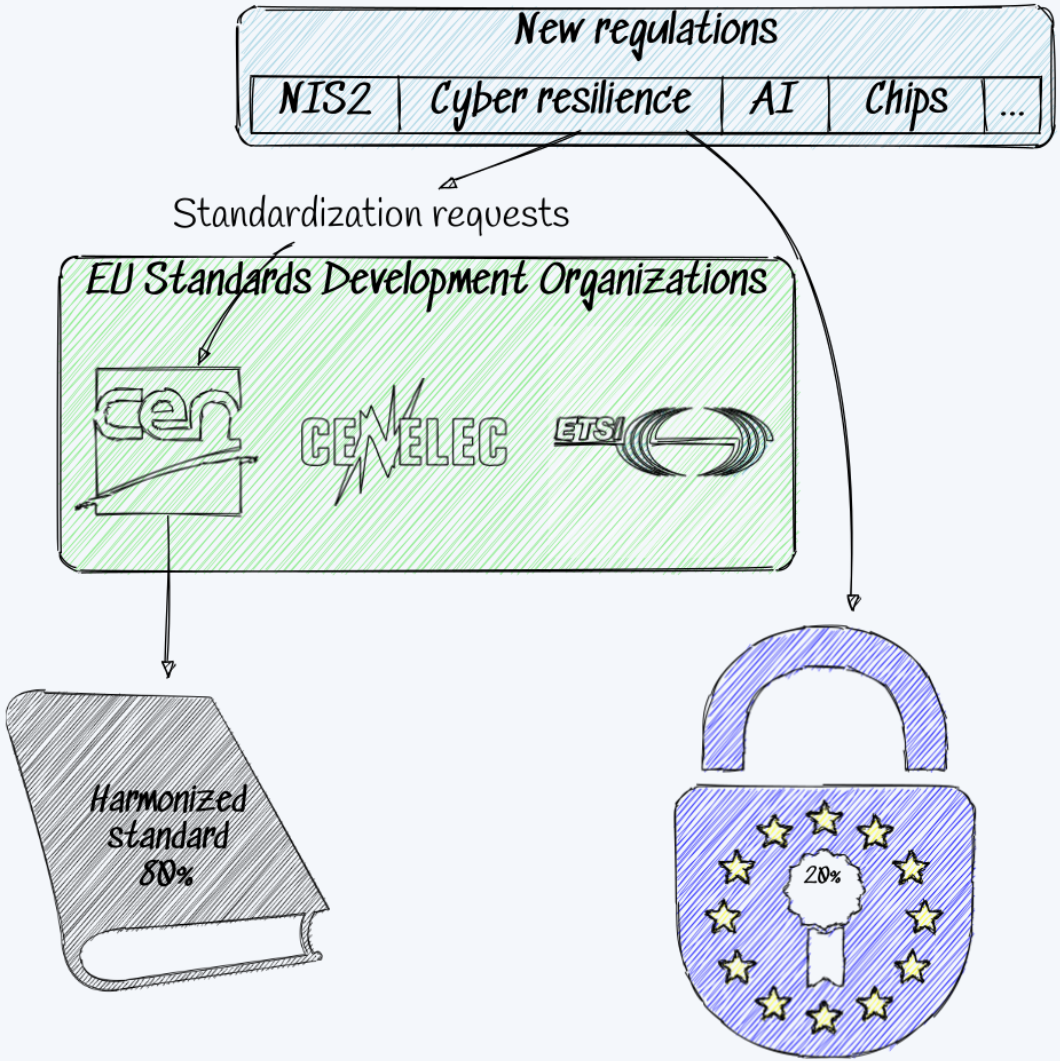
Which conformity assessment to follow?



Source: European Commission, DG CONNECT

European Commission

FORESEEABLE STANDARDS/CERTIFICATION LANDSCAPE IN EU MARKET


New regulations
NIS2
Cyber resilience
AI
Chips
...
Standardization requests
EU Standards Development Organizations
CEN
CENELEC
ETSI
Harmonized standard 80%
20%

THANKS!!