SNIA. STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Mandatory Cybersecurity Certification Requirements Coming of Age in the EU

Miguel Bañón

Table of Contents

- Abstract
- About the speaker
- References: EU legislation
- References: Cybersecurity certification
- Regulation (EU) 2019/881, Cybersecurity Act
- Next kid in town: European Cyber Resilience Act
- Global market and standards development

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, not just the critical infrastructures.

Industry-driven standardization initiatives have proven to be very successful in the past to provide to such legislative initiatives a solid body of work to be referenced. For the EUCC, for example, the payment sector was able to develop a comprehensive set of industry-agreed technical standards that are the bases of the high assurance certification in the EUCC. GSMA and 3GPP developed the NESAS certification scheme, which is currently under analysis for consideration as a building block of the EU5G.

This presentation analyses in more detail this scenario, and concludes with a call to the storage industry to participate in the development of cybersecurity standards.

About the speaker

Miguel Bañón has developed his career in the area of independent third party assurance, and has been contributing to cybersecurity standards development for more than 20 years. Former head of a Common Criteria and FIPS-140 2 evaluation and testing facility, he is currently Convenor of ISO/IEC JTC 1/SC 27/WG 3, where ISO/IEC 15408 and ISO/IEC 19790 are developed, of CEN/CLC JTC 13/WG 3, where standards are under development to support the new EUCS and EU5G, and member of the Management Board of the Common Criteria Users Forum.

IEC

1906 Award

The International Electrotechnical Commission
expresses its sincere appreciation of the valuable and sustainable contribution by

Miguel Bañón

Expert of the ISO/IEC JTC 1,
ISO/IEC Joint Technical Committee on information technology

Nominated by the Chair and Secretary of ISO/IEC JTC 1

In recognition for his leadership of JTC 1/SC 27/WG 3 in a very efficient and target oriented manner, and his very successful management of the important and complex liaison with the Common Criteria Board.

On behalf of the
International Electrotechnical Commission

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
- Commission invites citizens and organisations to share their views on the European Cyber Resilience Act

References: Cybersecurity certification

- Arrangement on the recognition of Common Criteria certificates in the field of Information Technology Security (CCRA)
- The National Information Assurance Partnership (NIAP)
- NIAP-approved Protection Profiles (PP)
- Common Criteria Users Forum
- ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security

Regulation (EU) 2019/881, Cybersecurity Act

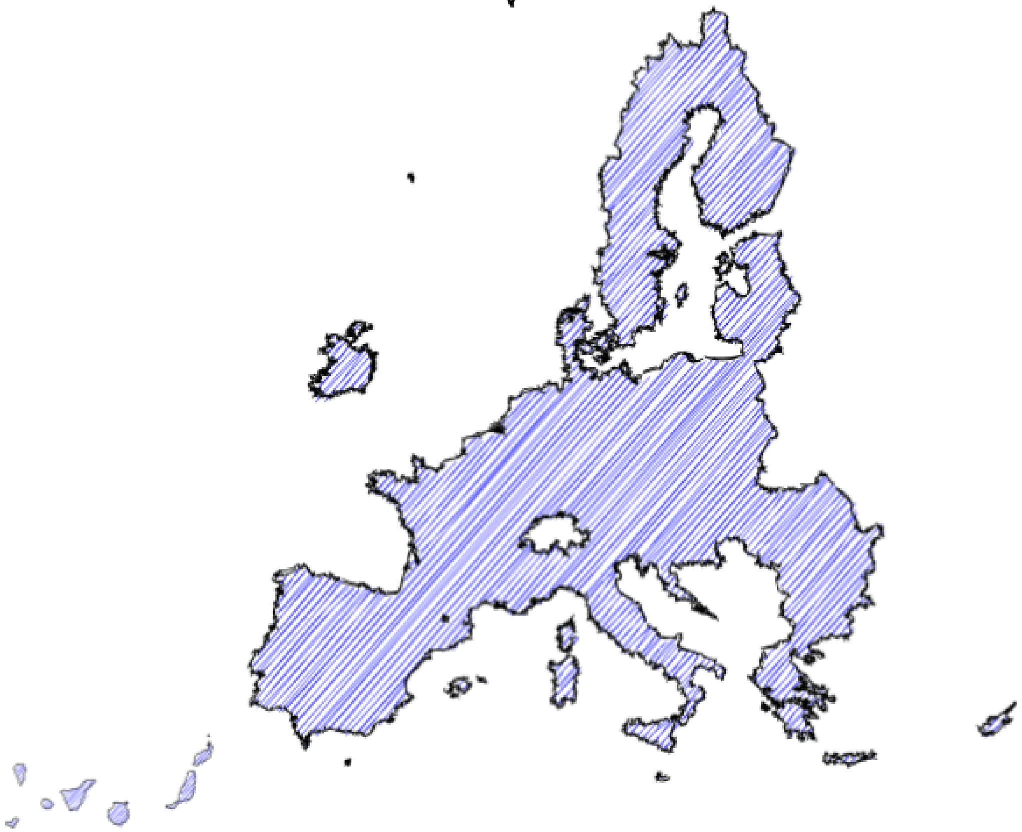
The CSA is a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with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

Regulation (EU) 2019/881
Cybersecurity Act

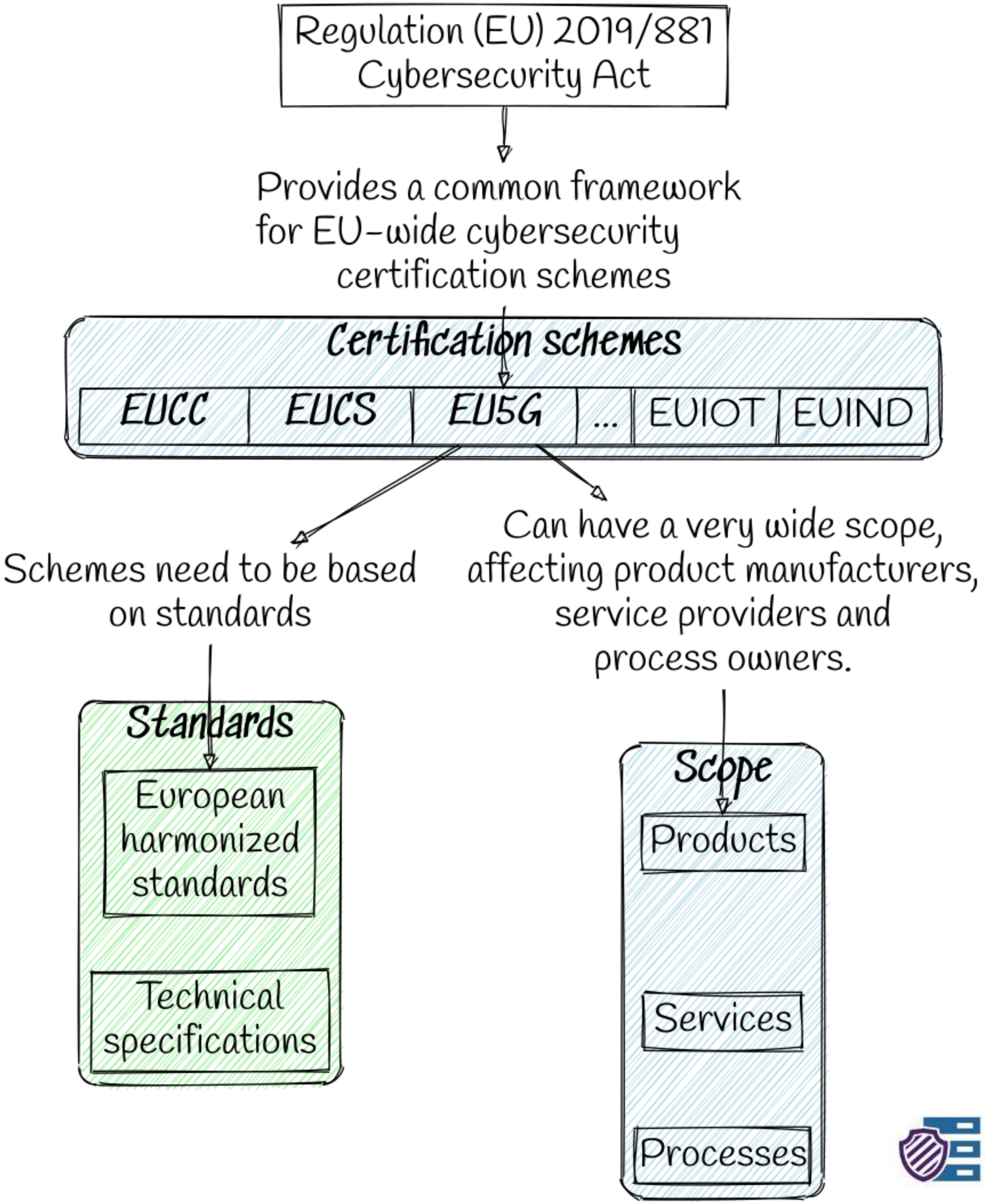
↓

Provides a common framework for EU-wide cybersecurity certification schemes

↓



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.



Regulation (EU) 2019/881
Cybersecurity Act

Provides a common framework for EU-wide cybersecurity certification schemes

Certification schemes

EUCC	EUCS	EU5G	...	EUIOT	EUIND

Schemes need to be based on standards

Can have a very wide scope, affecting product manufacturers, service providers and process owners.

Standards

- European harmonized standards
- Technical specifications

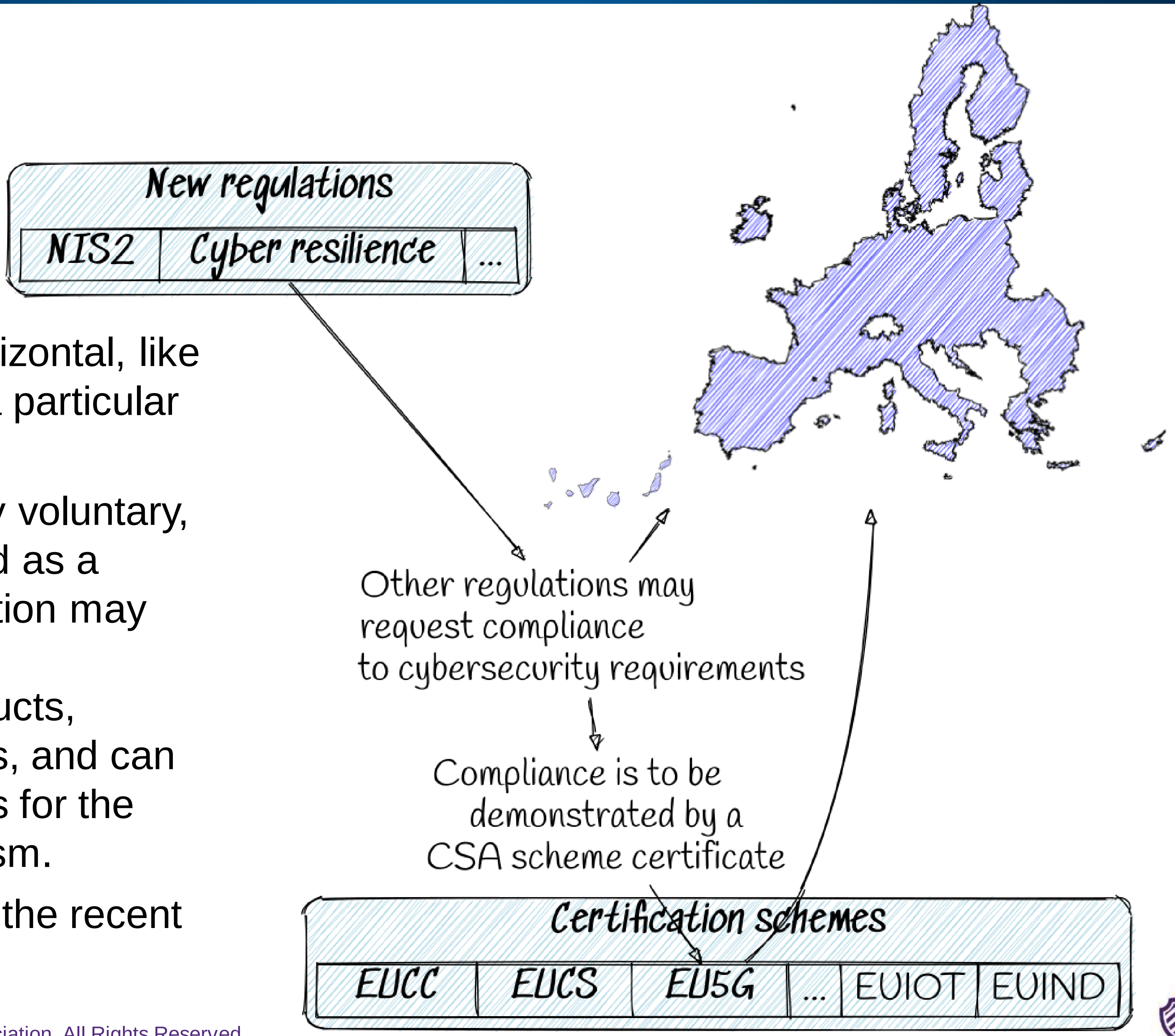
Scope

- Products
- Services
- Processes

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 clear example is the recent NIS2 proposal:



New regulations

NIS2	Cyber resilience	...

Other regulations may request compliance to cybersecurity requirements

Compliance is to be demonstrated by a CSA scheme certificate

Certification schemes

EUCC	EUCS	EU5G	...	EUIOT	EUIND

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.

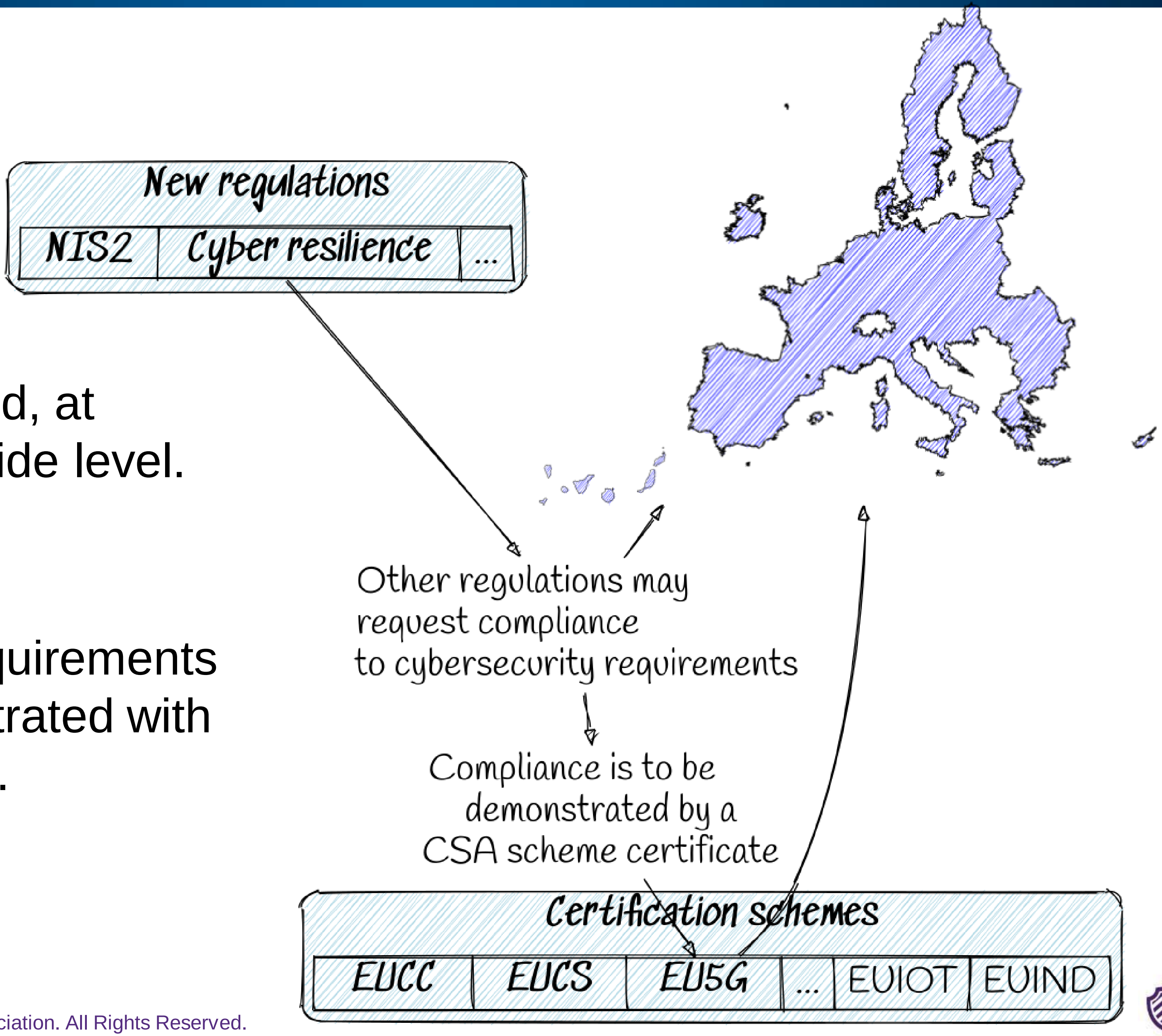
Article 21 ***Use of European cybersecurity certification schemes***

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 shall be demonstrated with a CSA certificate.



New regulations

NIS2	Cyber resilience	...

Other regulations may request compliance to cybersecurity requirements

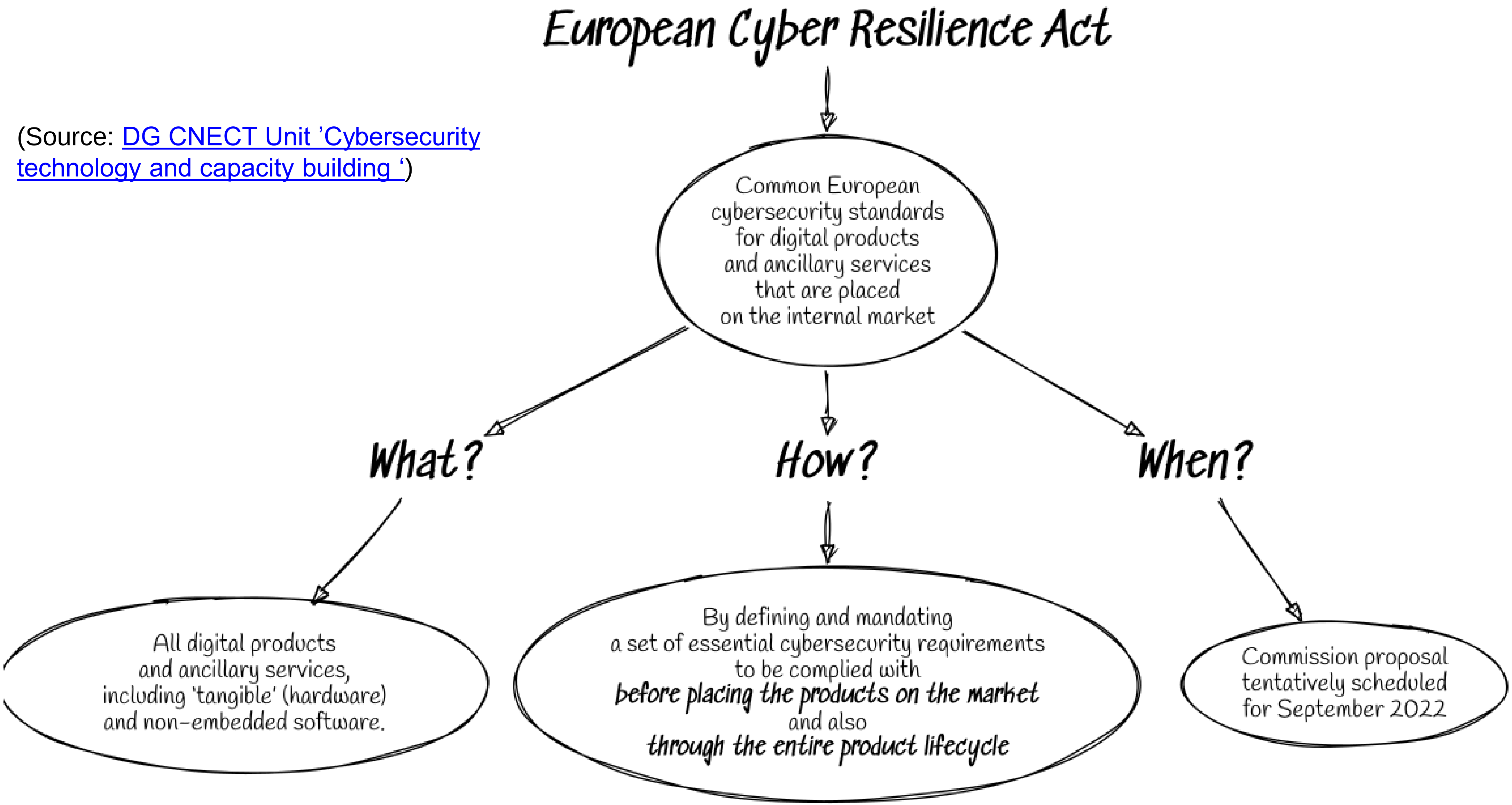
Compliance is to be demonstrated by a CSA scheme certificate

Certification schemes

EUCC	EUCS	EU5G	...	EUIOT	EUIND

Next kid in town: European Cyber Resilience Act

(Source: DG CNECT Unit ’Cybersecurity technology and capacity building ‘)



European Cyber Resilience Act

Common European cybersecurity standards for digital products and ancillary services that are placed on the internal market

What?

All digital products and ancillary services, including ‘tangible’ (hardware) and non-embedded software.

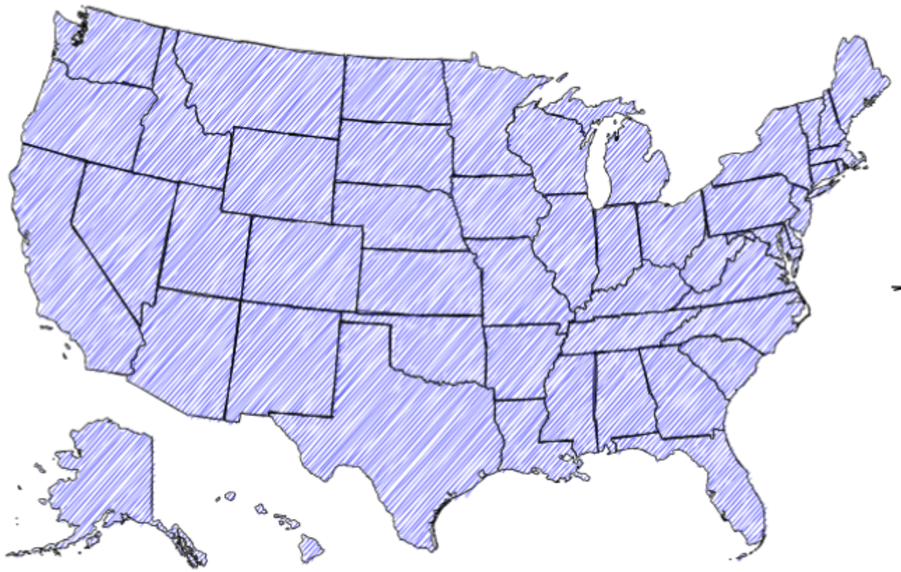
How?

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**

When?

Commission proposal tentatively scheduled for September 2022

Global market and standards development

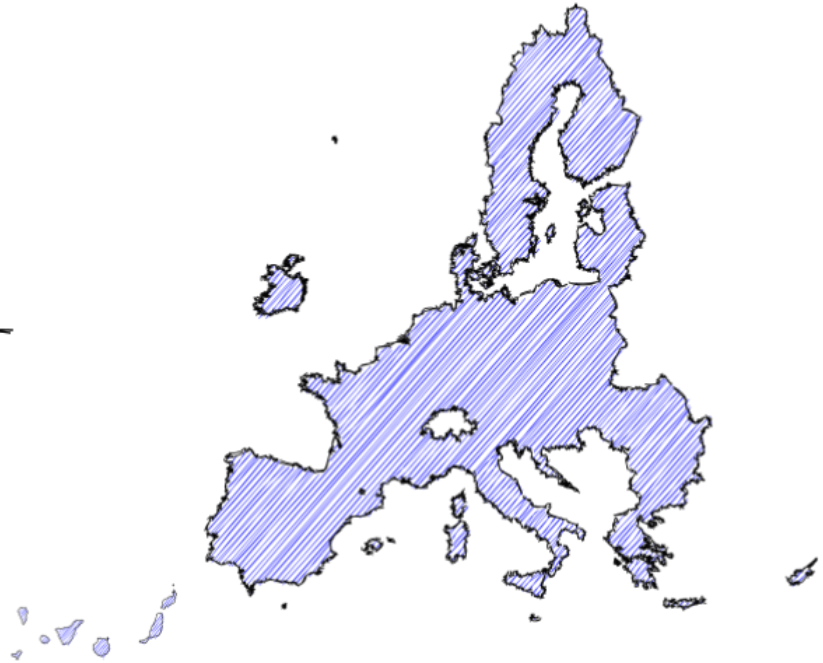


Mutual recognition

Common Criteria mutual recognition already existing.

Recognition with new EUCC under development.

Common Criteria



Achieving commonality of requirements and mutual recognition of certificates has been possible in the past based on high-quality standards.

NIAP manages a national program for developing Protection Profiles, evaluation methodologies, and policies that will ensure achievable, repeatable, and testable requirements.

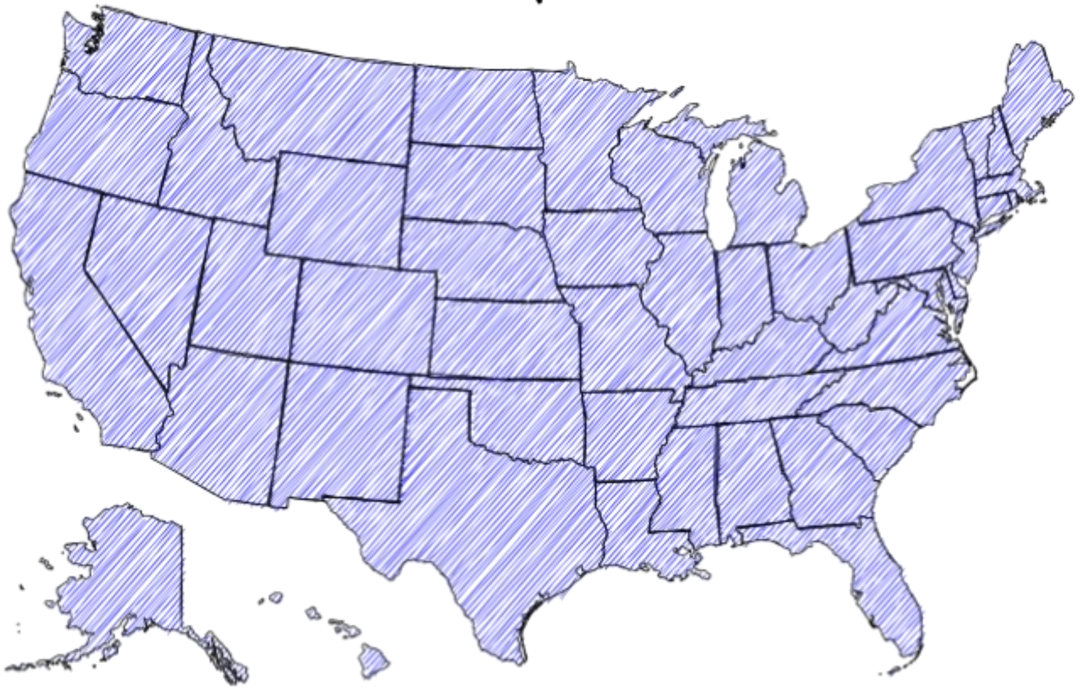
Products, evaluated and granted certificates by NIAP or under CCRA partnering schemes that comply with the requirements of the NIAP program and where applicable, the requirements of the Federal Information Processing Standard (FIPS) Cryptographic validation program(s) may be considered AS Complying with the Committee on National Security Systems Policy (CNSSP) 11, National Policy Governing the [Acquisition of Cybersecurity and Cybersecurity-Enabled Information Technology Products - dated June 2013]().

The U.S. National Information Assurance Partnership (NIAP)

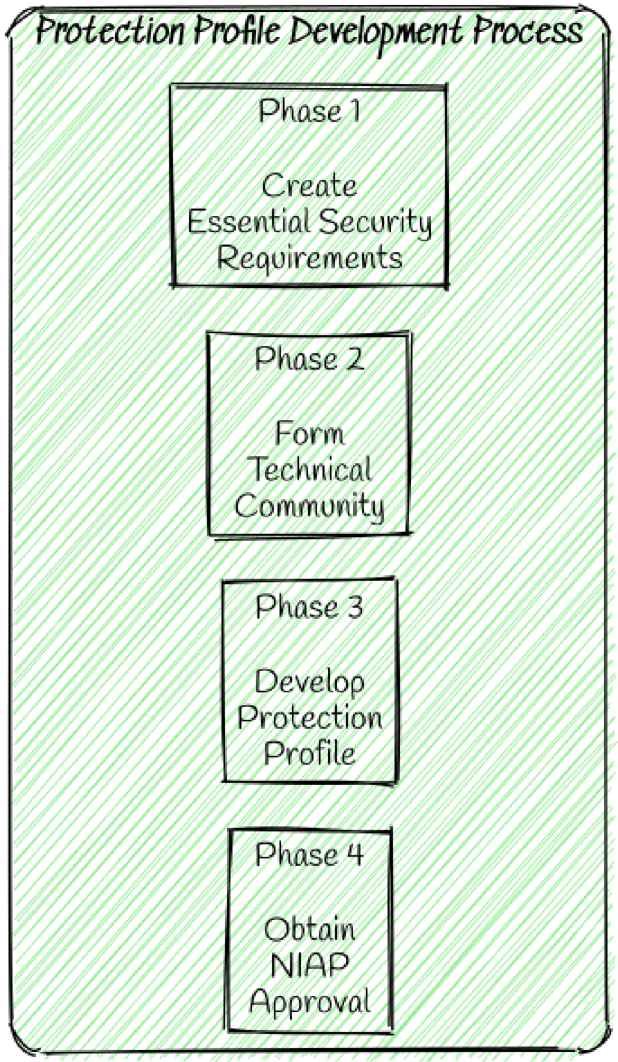
↓

Manages the compliance of U.S. Federal Administration Acquisition policies based on Common Criteria/FIPS 140-3 certificates

↓



Common Criteria



Protection Profile Development Process

Phase 1

Create Essential Security Requirements

Phase 2

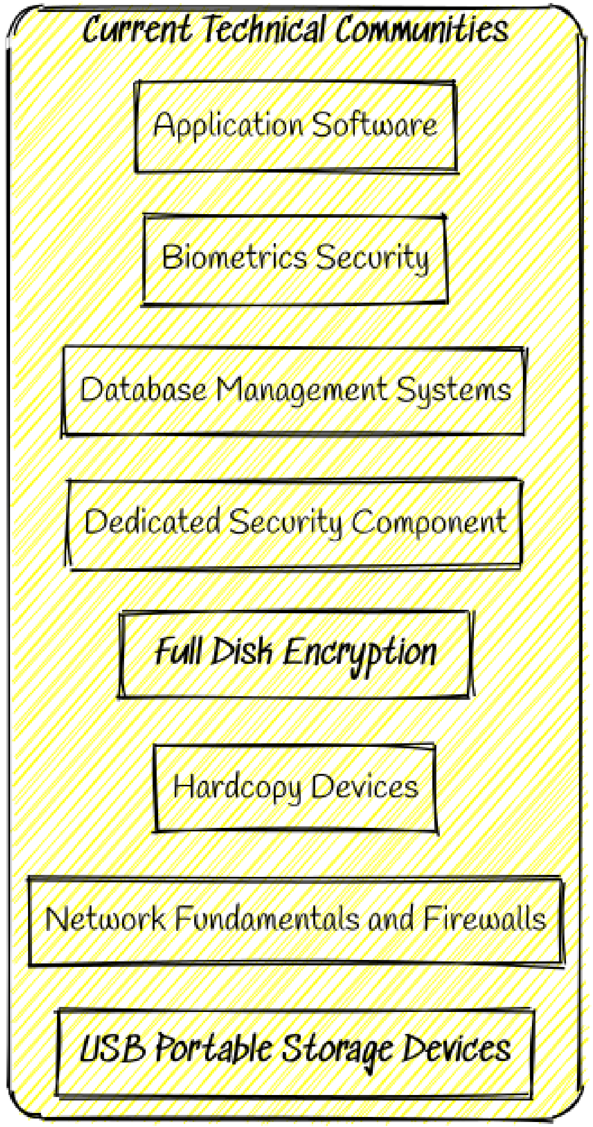
Form Technical Community

Phase 3

Develop Protection Profile

Phase 4

Obtain NIAP Approval



Current Technical Communities

Application Software

Biometrics Security

Database Management Systems

Dedicated Security Component

Full Disk Encryption

Hardcopy Devices

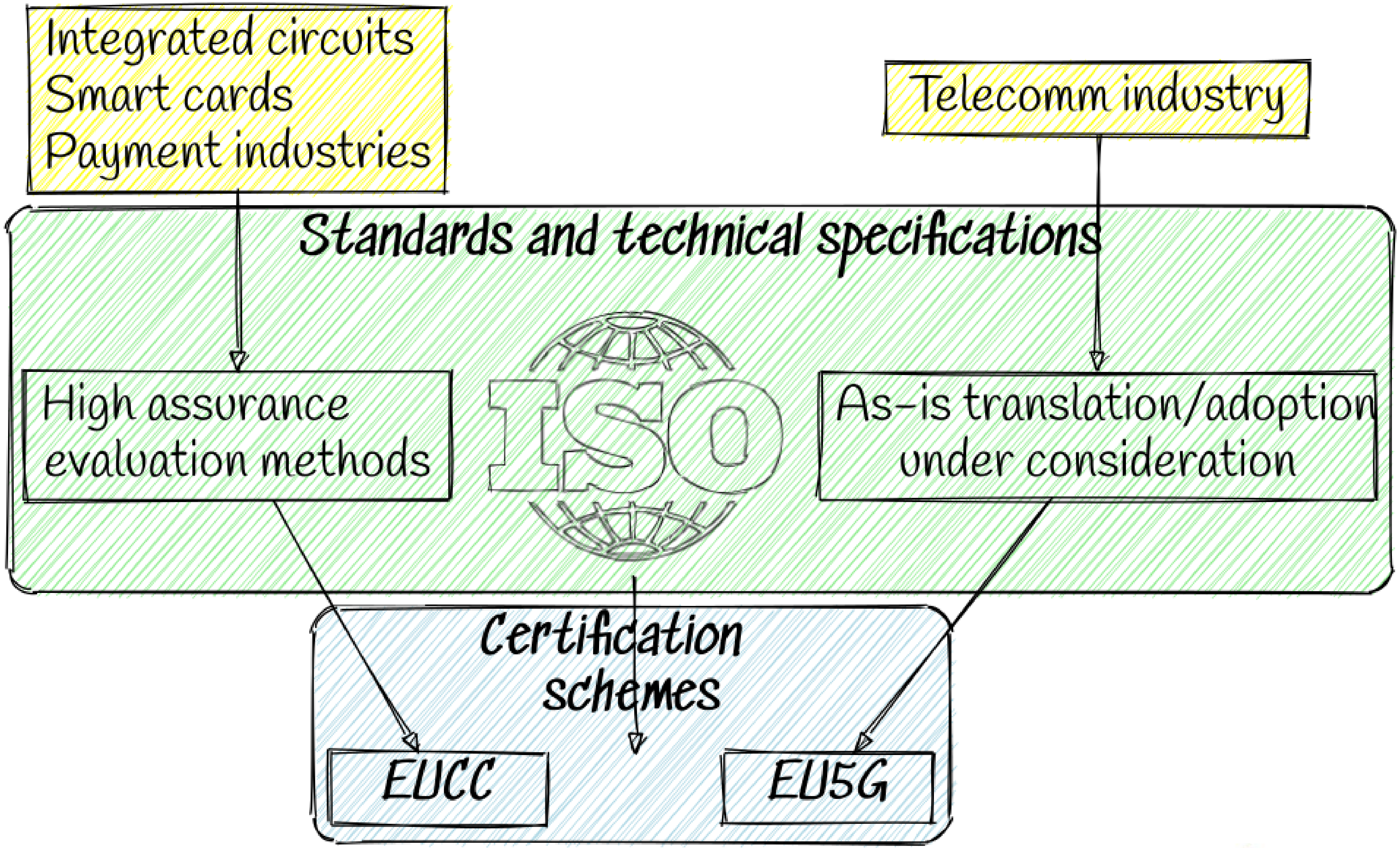
Network Fundamentals and Firewalls

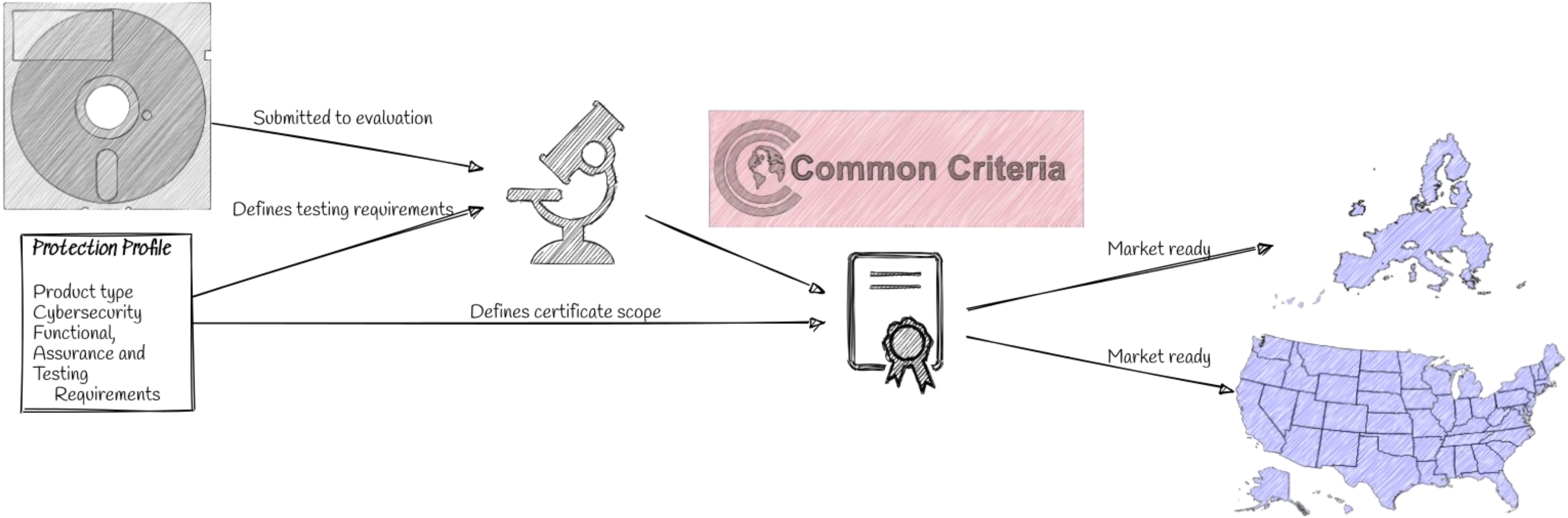
USB Portable Storage Devices

NIAP takes a collaborative approach to technology-specific protection profile development by supporting the creation of international technical communities of representatives from industry, government, end users, and academia.

It takes a considerable amount of time, effort and knowledge to develop useful standards.

The current EU schemes under development have been lucky to have industry-driven and mature cybersecurity requirements standards.


Integrated circuits
Smart cards
Payment industries
Telecomm industry
Standards and technical specifications
High assurance evaluation methods
ISO
As-is translation/adoption under consideration
Certification schemes
EUCC
EU5G



Submitted to evaluation

Defines testing requirements

Protection Profile

Product type
Cybersecurity
Functional,
Assurance and
Testing
Requirements

Defines certificate scope

Common Criteria

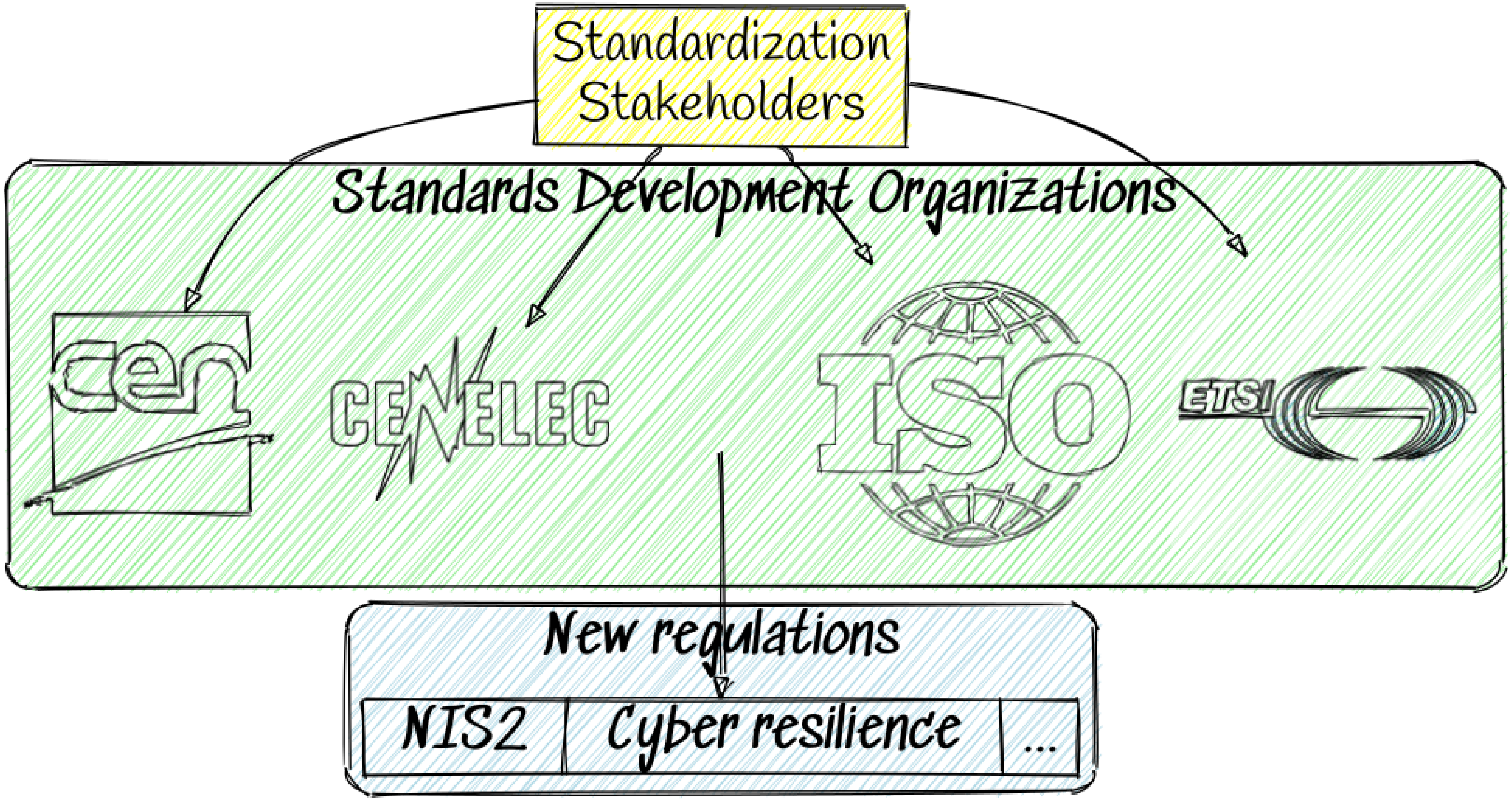
Market ready

Market ready

As markets mature in terms of cybersecurity, third-party assurance certification will become an entry bar, not just in the EU.

Standards are used to support legislation compliance.

Early investments and commitment from standardization stakeholders, including product manufacturers, in the development of such standards facilitate and speed-up the progressing of legislation, product cybersecurity and market acceptance.



Standardization Stakeholders
Standards Development Organizations
cen
CENELEC
ISO
ETSI
New regulations
NIS2
Cyber resilience
...

Standards Development

We need

Y U

Thanks!!