Standards for new requirements on digital products

Mapping Cyber Resilience Act requirements against Cyber Security Standards

A joint JRC-ENISA Study

Igor Nai Fovino, Ph.D.

Deputy Head of Unit

Cybersecurity and Digital Technologies Capabilities Unit

Joint Research Centre - European Commission

European Commission

CRA Proposal Requirements – general principles

Section 1: security requirements relating to the properties of products with digital elements

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**

(b) ensure protection **from unauthorised access**

(c) protect the **confidentiality of stored, transmitted or otherwise processed data**, … **by state of the art mechanisms;**

(d) protect **the integrity** of stored, transmitted or otherwise processed data

(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 (incl. from **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**

(i) be designed, developed and produced to **reduce the impact** of an incident

(j) provide security related information by recording and/or **monitoring relevant internal activity**

(k) ensure that vulnerabilities can be addressed through **security updates**

Section 2: vulnerability handling requirements

Manufacturers of the products with digital elements shall:

(1) **Identify and document vulnerabilities** and components contained in the product

(2) **Address and remediate vulnerabilities** without delay, including by providing **security updates**;

(3) Apply **effective and regular tests and reviews of the security of the product**

(4) Once a security update has been made available, **publically disclose information about fixed vulnerabilities**

(5) Put in place and enforce a policy on **coordinated vulnerability disclosure**;

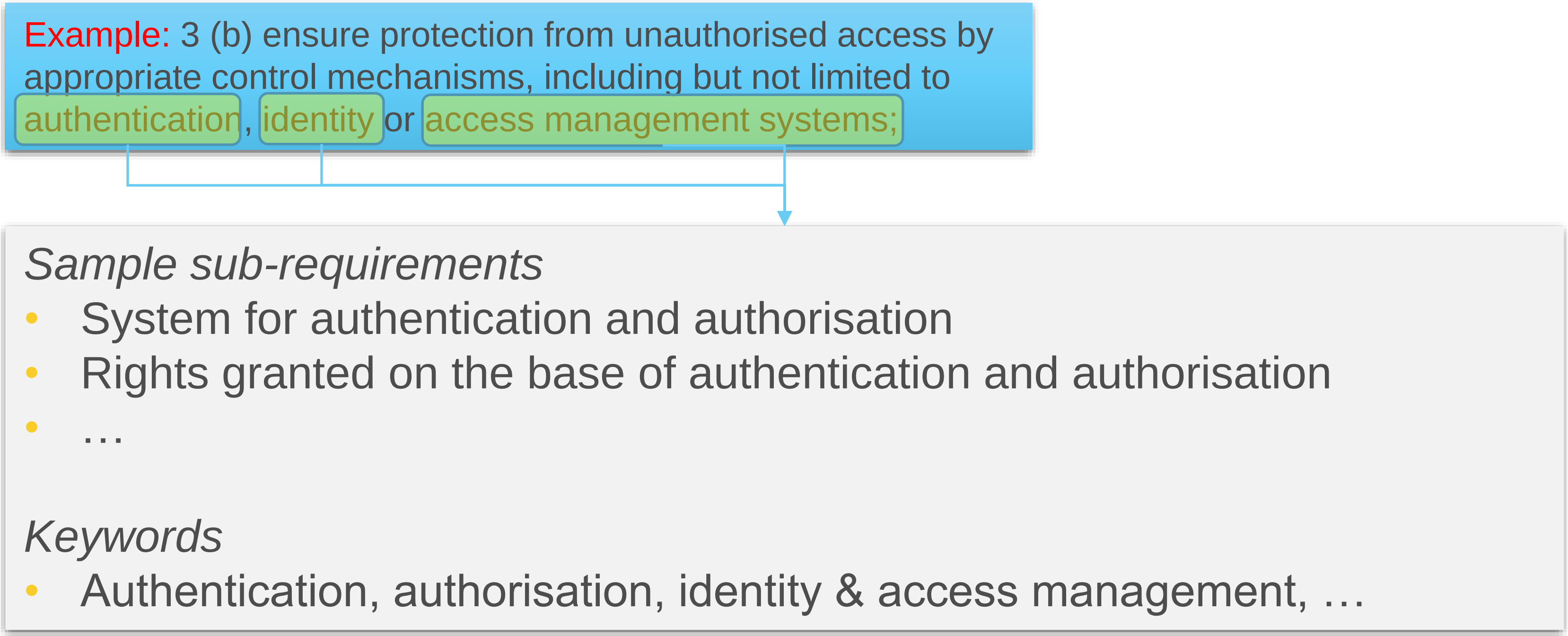
(6) Take measures to facilitate **the sharing of information about potential vulnerabilities**

(7) Provide for mechanisms to **securely distribute updates** for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) Ensure that, where security patches or updates are available to address identified security issues, they are **disseminated without delay and free of charge**, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Understanding the Requirements

CRA Requirements are High Level Requirements



Example: 3 (b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

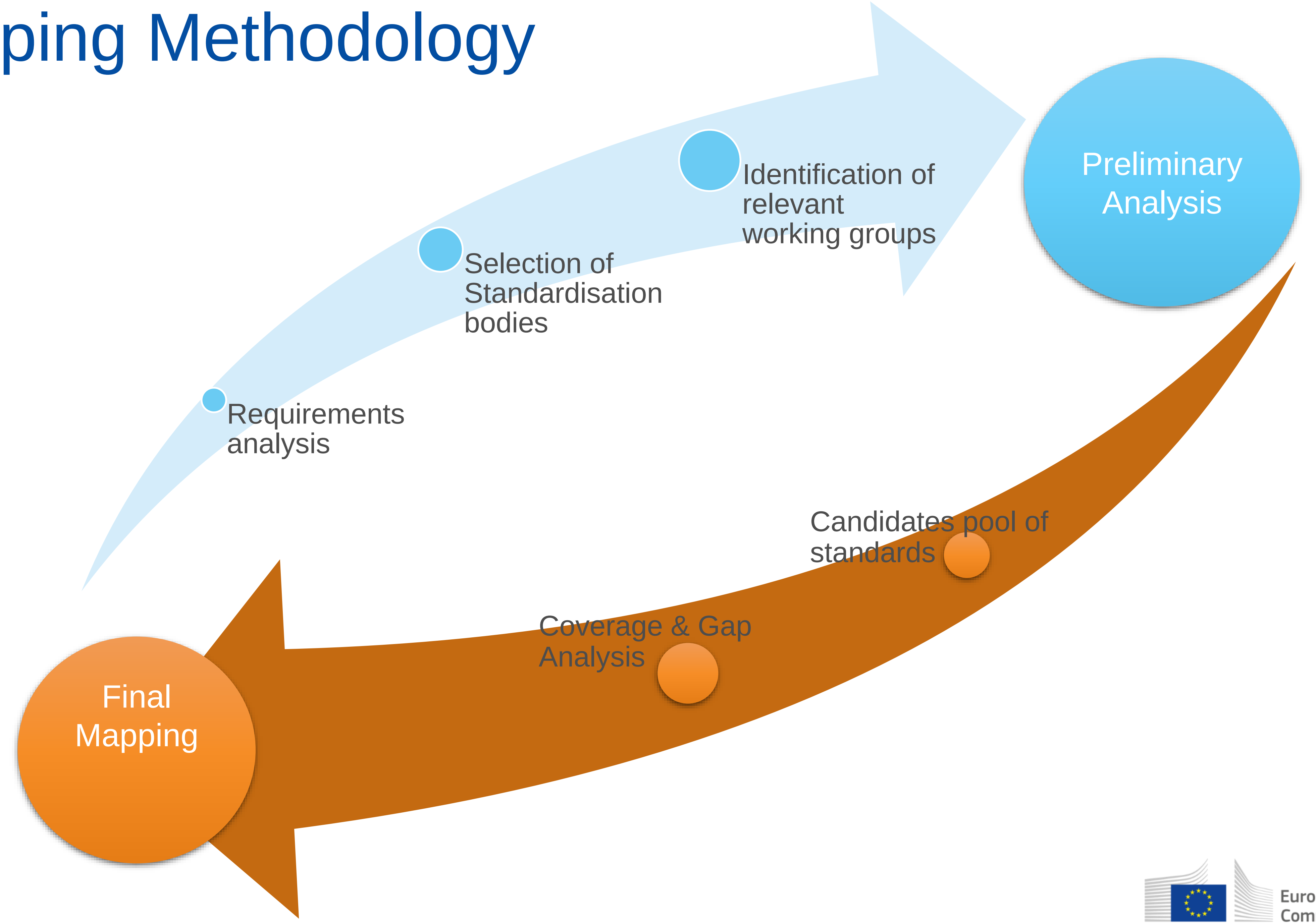
Sample sub-requirements

- System for authentication and authorisation
- Rights granted on the base of authentication and authorisation
- …

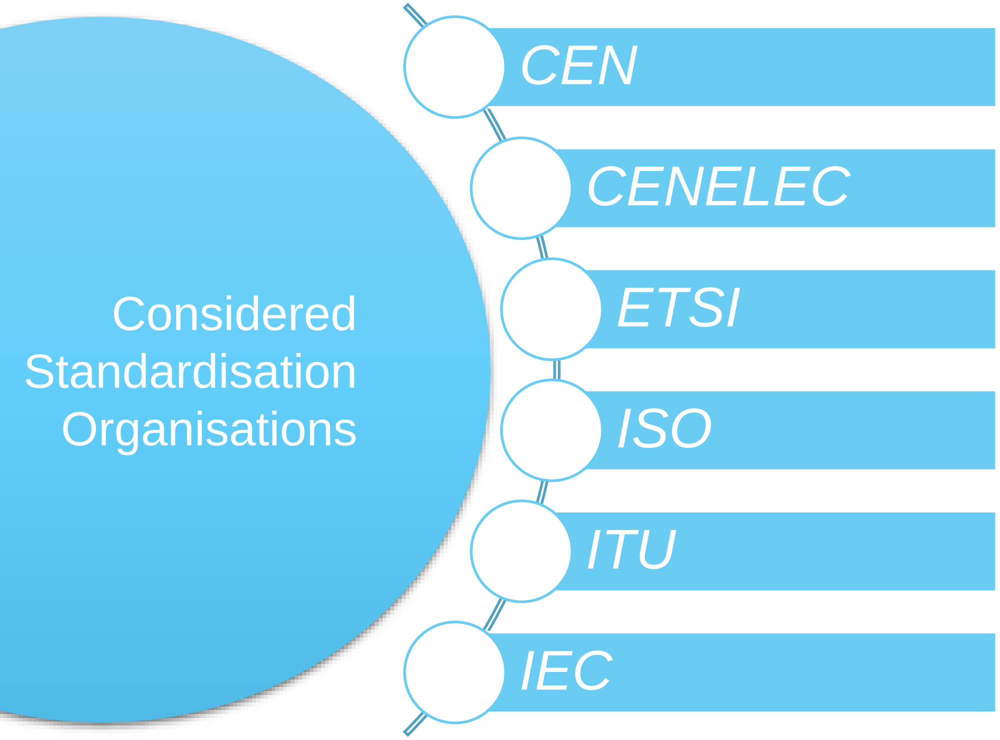
Keywords

- Authentication, authorisation, identity & access management, …

Mapping Methodology

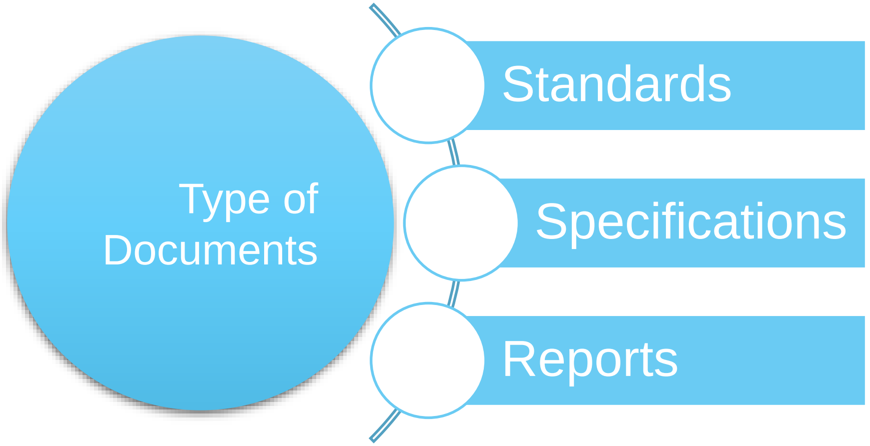

Preliminary Analysis
Requirements analysis
Selection of Standardisation bodies
Identification of relevant working groups
Candidates pool of standards
Coverage & Gap Analysis
Final Mapping

Preliminary Analysis in numbers



Considered Standardisation Organisations

- *CEN*
- *CENELEC*
- *ETSI*
- *ISO*
- *ITU*
- *IEC*



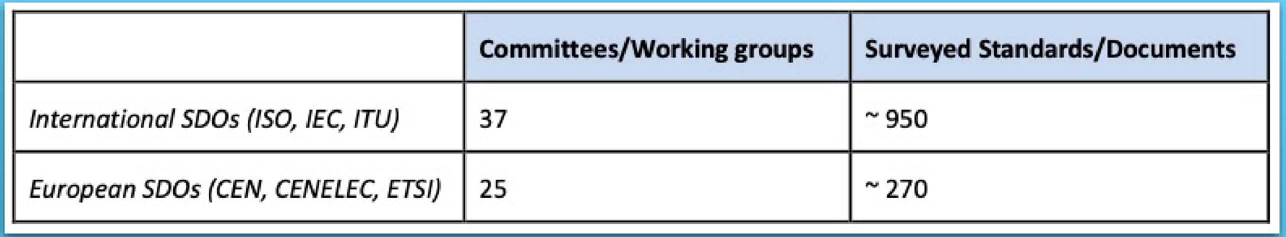
Type of Documents

- Standards
- Specifications
- Reports

Priority to standards and specifications (Prescriptive vs Descriptive)

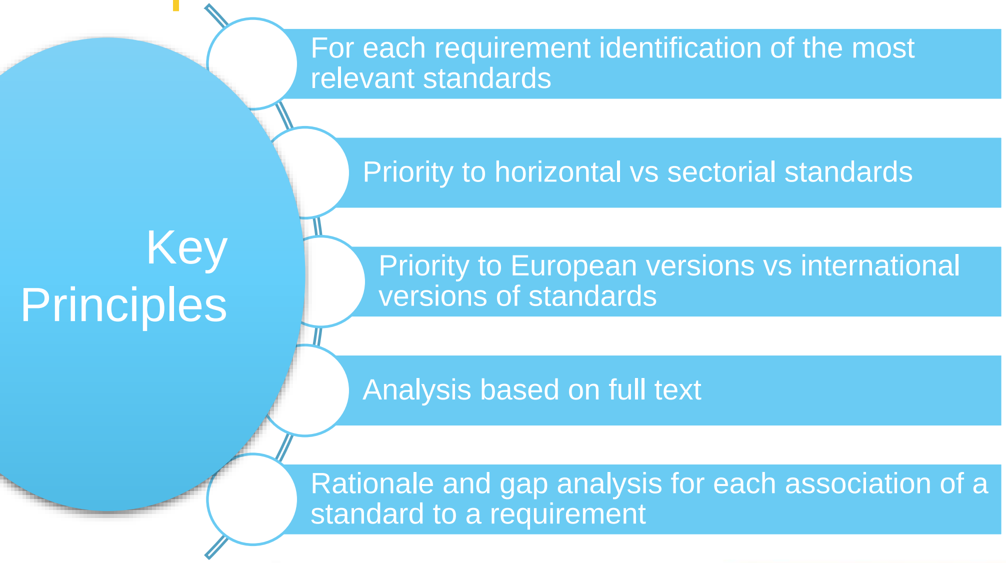
Identified and surveyed:

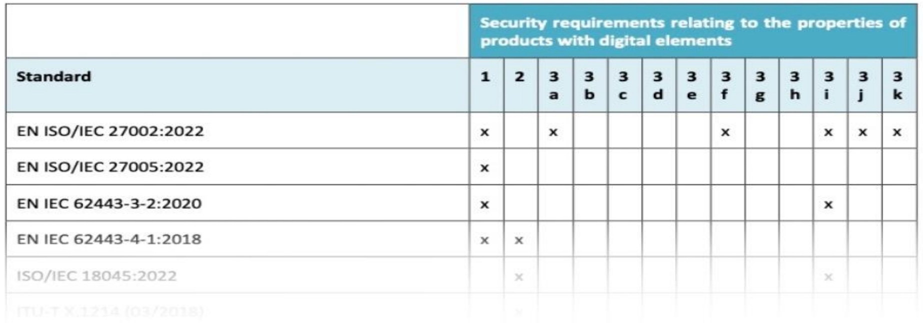
- activities of more than 60 committees/working groups



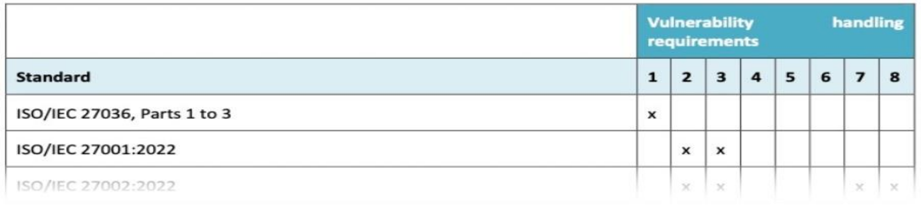
	Committees/Working groups	Surveyed Standards/Documents
International SDOs (ISO, IEC, ITU)	37	~ 950
European SDOs (CEN, CENELEC, ETSI)	25	~ 270

Mapping and gap analysis

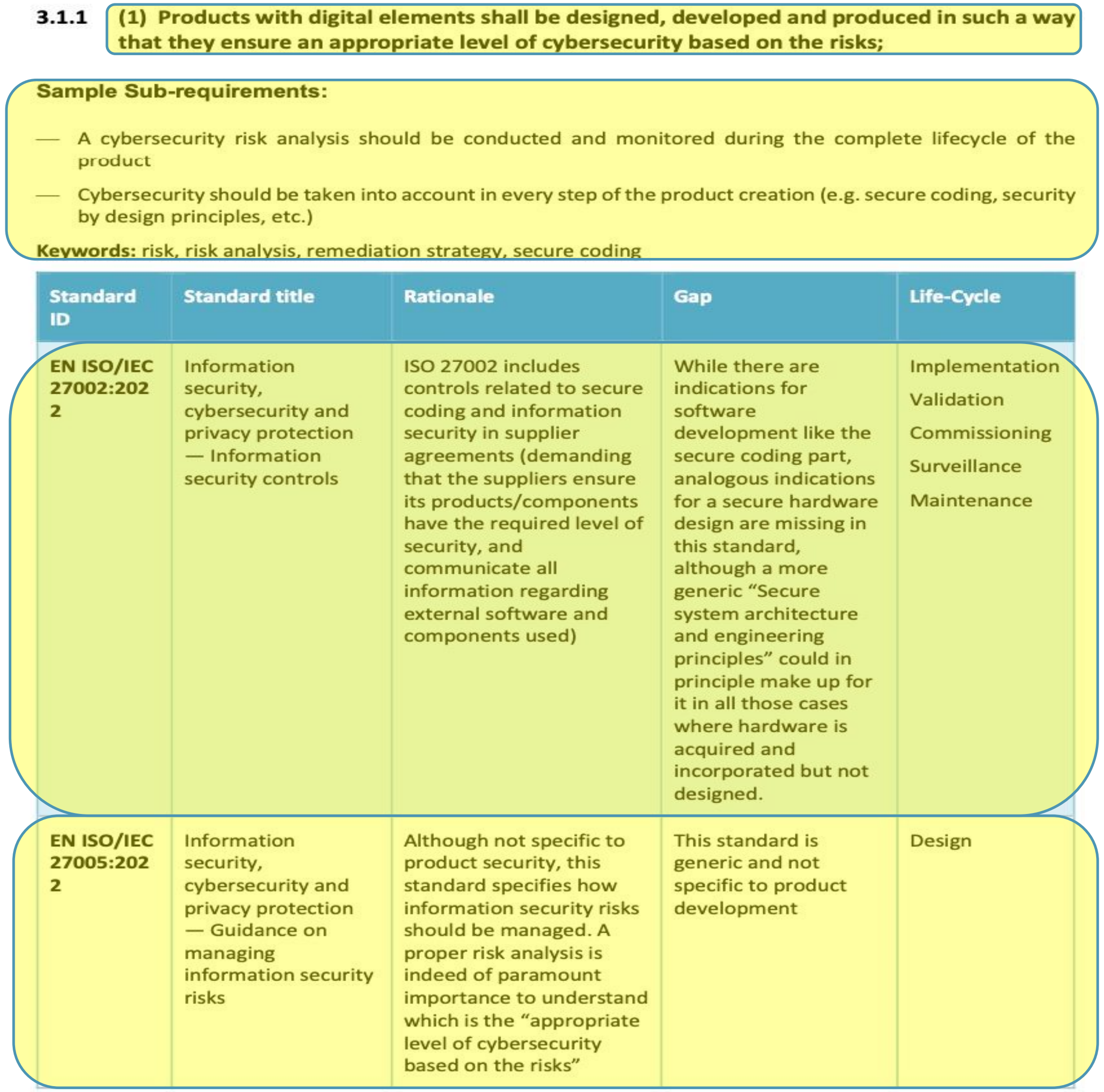

Key Principles
For each requirement identification of the most relevant standards
Priority to horizontal vs sectorial standards
Priority to European versions vs international versions of standards
Analysis based on full text
Rationale and gap analysis for each association of a standard to a requirement



	Security requirements relating to the properties of products with digital elements												
Standard	**1**	**2**	**3 a**	**3 b**	**3 c**	**3 d**	**3 e**	**3 f**	**3 g**	**3 h**	**3 i**	**3 j**	**3 k**
EN ISO/IEC 27002:2022	x		x					x			x	x	x
EN ISO/IEC 27005:2022	x												
EN IEC 62443-3-2:2020	x										x		
EN IEC 62443-4-1:2018	x	x											
ISO/IEC 18045:2022		x									x		
ITU-T X.1214 (03/2018)		x											



	Vulnerability handling requirements							
Standard	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
ISO/IEC 27036, Parts 1 to 3	x							
ISO/IEC 27001:2022		x	x					
ISO/IEC 27002:2022		x	x				x	x



3.1.1 **(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;**

Sample Sub-requirements:

— A cybersecurity risk analysis should be conducted and monitored during the complete lifecycle of the product

— Cybersecurity should be taken into account in every step of the product creation (e.g. secure coding, security by design principles, etc.)

Keywords: risk, risk analysis, remediation strategy, secure coding

Standard ID	Standard title	Rationale	Gap	Life-Cycle
EN ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection — Information security controls	ISO 27002 includes controls related to secure coding and information security in supplier agreements (demanding that the suppliers ensure its products/components have the required level of security, and communicate all information regarding external software and components used)	While there are indications for software development like the secure coding part, analogous indications for a secure hardware design are missing in this standard, although a more generic "Secure system architecture and engineering principles" could in principle make up for it in all those cases where hardware is acquired and incorporated but not designed.	Implementation Validation Commissioning Surveillance Maintenance
EN ISO/IEC 27005:2022	Information security, cybersecurity and privacy protection — Guidance on managing information security risks	Although not specific to product security, this standard specifies how information security risks should be managed. A proper risk analysis is indeed of paramount importance to understand which is the "appropriate level of cybersecurity based on the risks"	This standard is generic and not specific to product development	Design

Few Considerations (1)

- The existing standards cover at least partially all CRA requirements.
- **Not a single standard, alone,** can satisfy all requirements listed in the Annex I of the CRA;
- “**Horizontal” standards** - i.e., not targeting a specific use case or a market sector/product - emerged as the most relevant to cover the purposes of the different requirements.
- The only exception to this is represented by some standards of the **EN IEC 62443 family** (related to industrial control systems) and the Internet of Things (IoT)

Few Considerations (2)

- Regarding the product-related security requirements of the first list of CRA Annex I, the standard ETSI EN 303 645 somehow covered the requirements (even if at very high level), with some gaps.

- Another relevant standard in terms of coverage of the requirements is EN ISO/IEC 27002 (information security controls), covering 6 out of 13 requirements.

- For the vulnerability handling requirements, EN ISO/IEC 30111 (vulnerability handling process) is the most relevant one, covering 5 out of 8 requirements, with also EN ISO/IEC 29147 (vulnerability disclosure) covering 4 of the same requirements. All these standards are “horizontal” in terms of their application;

Few Considerations (3)

Duality between horizontal high level and sectorial low level… Three examples

- In some cases, such as requirement 3(b) (ensure protection from unauthorised access…), the selected standards are quite **generic** whereas there exist several other standards covering specific use cases in more detail

- In other cases, e.g., 3(f) (protect the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks), the focus of the identified standards is more on infrastructural elements rather than user products or services. --> **more specific standard provisions would be needed**.

- While requirement 3(g), which focuses on minimizing negative impacts on the availability of services provided by other devices or networks, is specifically addressed by standards related to the IoT domain, questions exist on the use of this standards for non-IoT related

Final Remarks

- All requirements are at least partially covered by a standard
- The “Universal Standard” for the CRA does not exist today
- There is however a good existing base for future standardisation activities despite gaps
- Duality between horizontal and vertical standards is not a burden, but an added value and an occasion make something new, more agile and effective .

Thank you