Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

This is a **Guide** about the

EU Cyber Resilience Act.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

About the project

This Guide has been designed and developed in the context of the 'EcoCyber' project, carried out within the SERICS Extended Partnership, a national initiative under the MUR National Recovery and Resilience Plan funded by the European Union Next Generation EU.

The project 'EcoCyber – Risk Management for Future Cyber-Physical Ecosystems' is devoted to advancing innovative technical and legal solutions and methods **to leverage the opportunities offered by cyber-physical systems while addressing the relevant connected challenges** (e.g., cyber threats and vulnerabilities).

In particular, **this work has been conducted by the research teams from two Work Packages of EcoCyber**: WP 2 (Solutions for the design and testing of secure smart components) and WP 4 (Rules for the future society), integrating therefore technical and legal aspects.

Finanziato dall'Unione Europea - NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 - Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca - D. D. 341 del 15/03/2022, PE7 SERICS - SEcurity and RIghts in the CyberSpace , Codice proposta: PE00000014, CUP: J33C22002810001, finanziato con Decreto n. 1556 del 11/10/2022

Team

Pier Giorgio Chiara
Cybersecurity legal expert

Alessandro Vannini
OT cybersecurity engineer

Geordie Morciano
Legal designer

Raffaella Brighi
Coordinator

Marco Prandini
Coordinator

Ver 1.0, 11-12-2025

Methodology

The Guide was developed through an innovative, multidisciplinary methodology that integrates **legal design principles** with **technical expertise in cybersecurity and information technology**.

The project team, comprising an EU cybersecurity law expert, a legal design specialist, and an engineer specialized in Operational Technology (OT) security, adopted the **design thinking process** as its operational framework.

This approach, structured around the phases of needs analysis, ideation, prototyping, and validation, enabled the systematic integration of legal, technical, and communicative perspectives into a single, coherent workflow.

- The result is **a Guide that translates the CRA's regulatory complexity into accessible, operational, and legally sound content, supporting consistent and effective application across professional and organizational contexts.**
- The **Guide** aims to provide **operational and interpretive guidance** for the **parties** involved, **including relevant economic operators, legal advisors, and cybersecurity IT expert**

Design thinking process

Research

Identification of user needs through structured interviews and data analysis, leading to the creation of representative user profiles.

Definition & Ideation

Translation of insights into concrete design solutions using collaborative methods to organize CRA content into a clear, usable structure.

Prototyping

Development of an interactive visual-textual document that simplifies regulatory and technical requirements.

User Testing

Evaluation of the prototype by professionals from various fields; feedback informs revisions and improvements.

Refinement & Launch

Final adjustments based on testing results and publication of the completed Guide.

What is the focus of the Guide

Cyber Resilience Act

Chapter I	**Arts. 1-12**	**General provisions**
II	**Arts. 13-26**	**Obligations of economic operators** and provisions in relation to **free and open-source software**
III	**Arts. 27-34**	**Conformity of the PDEs**
IV	Arts. 35-51	Notification of conformity assessment bodies
V	Arts. 52-60	Market surveillance and enforcement
VI	Arts. 61-62	Delegated powers and committee procedure
VII	**Arts. 63-65**	**Confidentiality and penalties**
VIII	**Arts. 66-71**	**Transitional and final provisions**

Commission Implementing Regulation (EU) 2025/2392

Technical description of important and critical products

Commission FAQ December 2025

Scope of the Guide

The Cyber Resilience Act (CRA) is structured into eight Chapters and several Annexes.

This project focuses specifically on Chapters I to III and Chapter VII, which address penalties.

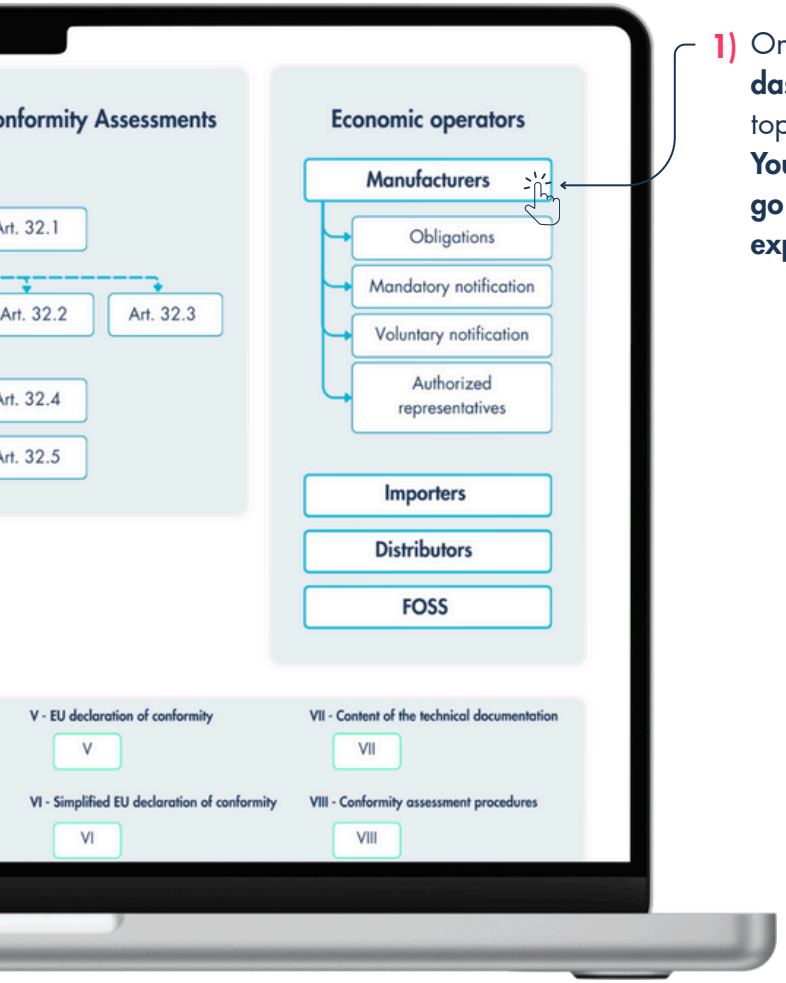
These sections are identified as the **most relevant** and **operationally significant for the end users** of the Guide, who are directly involved in applying the Regulation.

For this reason, **other provisions**, such as Arts. 1,9,10,33 and 34 **have not been included, as they were not considered as a priority for this Guide**.
Consequently, the following pages do not strictly follow the numerical order of the Regulation's articles; instead, they are **organised in a logical structure that highlights the conceptual connections** between the selected provisions.

Additional useful information to assist stakeholders in implementing the CRA **has been integrated with the official text of the Regulation**.

How to use this document

This Guide is designed to be interactive and easy to navigate.
Colored sections and visual markers help users move quickly between related topics and access information that appears in different parts of the document.
By clicking on these sections, you can jump directly to the relevant content without losing the overall context.



1) On the next page, you will find the **dashboard**, a kind of map of all the topics covered in this Guide.
You can click on any specific topic to go directly to the page where it is explained.

2) In this bar, you will find the **specific topic of the Article explained** in the visual boards.

3) Use this button to **return to the dashboard**.

4) Use this button to **go back** to the last page you viewed.

5) By clicking on one of these boxes, you will be directed to the **page containing the detailed explanation of the referenced topic**.

Art. X

Example

6) This icon ⓘ indicates information taken from the **European Commission's FAQs** and provides interpretative guidance.
When you hover over it, a popup will appear with additional details.

7) The number of **the Article or section covered** in this section is shown below.

Legend

This is a dashboard: click on the section you want to explore further

General

- **Timing**
- **Penalties**

Products

- **PDEs in scope**
  - Default
  - Important
  - Critical
  - FOSS
- High-risk AI systems
- PDEs **out** of scope
- **Requirements**

Conformity Assessment

- **Technical documentation**
  - Art. 32.1
  - Art. 32.2
  - Art. 32.3
  - Art. 32.4
  - Art. 32.5
- **Presumption of conformity**
- **EU declaration of conformity**
- **CE marking**

Economic operators

- **Manufacturers**
  - **Obligations**
  - **Mandatory** notification
  - **Voluntary** notification
  - Authorized representatives
- **Importers**
- **Distributors**
- **FOSS**
  - **Stewards**
  - **Security attestation**

PDEs > Products with Digital Elements

FOSS > Free and Open-Source Software

Annex

I - Essential cybersecurity requirements

I, part 1 | I, part 2

II - Information and instructions to the user

II

III - Important PDEs

III, class 1 | III, class 2

IV - Critical PDEs

IV

V - EU declaration of conformity

V

VI - Simplified EU declaration of conformity

VI

VII - Content of the technical documentation

VII

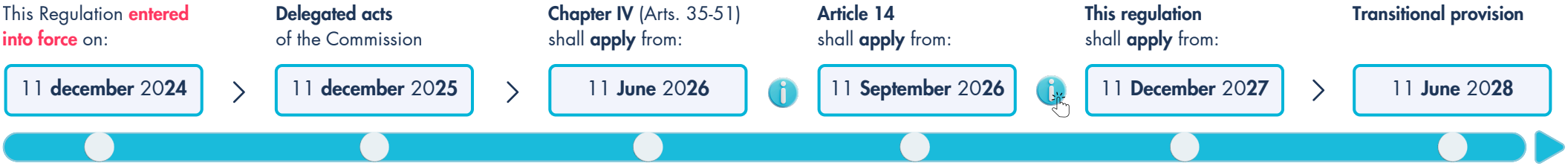
VIII - Conformity assessment procedures

VIII

Regulation timeline

This timeline highlights key dates expressly set out in the text of the Cyber Resilience Act (CRA).

Each date marks a specific step in the gradual implementation of the CRA framework - from its entry into force to its full legal application across the EU market. They represent important milestones for manufacturers, importers, distributors, and technical professionals to consider in **planning and maintaining compliance** with the Regulation.



The CRA becomes EU law. The countdown to compliance begins.
Art. 71.1

By this date, the Commission adopts an implementing act **specifying the technical description of "important" and "critical" PDEs**.
Art. 7.4

On the same date, it also adopts delegated acts specifying the **terms and conditions for applying cybersecurity-related grounds** for delaying the dissemination of notifications as referred to Art.16(2).
Art. 14.4

Rules on notification of conformity assessment bodies start applying.
Art. 71.2

Start of reporting duties: **once Article 14 of the CRA applies**, manufacturers must report exploited vulnerabilities and severe incidents (Art. 71.2), **even if** that PDE has been placed on the market **before 11 December 2027.**
Art. 69.3

Full application: the CRA applies in full to all products placed on the EU market.
Art. 71.2

PDEs that have been placed on the market **before 11 December 2027** shall be subject to the requirements set out in this Regulation **only if, from that date, those products are subject to a substantial modification.**
Art. 69.2

EU type-examination certificates and **approval decisions** issued regarding cybersecurity requirements for PDEs **that are subject to Union harmonisation legislation other than the CRA** remain **valid until this date, unless they expire before** or otherwise specified in the applicable Union harmonisation legislation.
Art. 69.1

Example

Who must comply?

'**Economic operator**' which means the manufacturer, the authorised representative, the importer, the distributor, **or other natural or legal person who is subject to obligations** in relation to the manufacture of products with digital elements (PDEs) or to the making available of PDEs on the market in accordance with this Regulation.
Art. 3(12)

Art. 23: **Identification of economic operators**

Manufacturer

natural or legal person who develops or manufactures PDEs or has PDEs designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge.
Art. 3.13

Importer

natural or legal person established in the Union who places on the market a PDEs that bears the name or trademark of a natural or legal person established outside the Union.
Art. 3.16

Distributor

natural or legal person in the supply chain, other than the manufacturer or the importer, **that makes a PDEs available on the Union market** without affecting its properties.
Art. 3.17

Open-source software developer

legal person, other than a manufacturer, **that has the purpose or objective of systematically providing support on a sustained basis for the development of specific PDEs, qualifying as free and open-source software** and intended for commercial activities, and that ensures the viability of those products.
Art. 3.14

Authorised representative

natural or legal person established within the Union **who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks**.
Art. 3.15.

21

An importer or distributor is **considered to be a manufacturer**, where they place a PDEs on the market
- **under its name or trademark, or**
- carry out a **substantial modification** of a PDEs already placed on the market.

And they shall be **subject to Arts. 13 and 14**.

Art.13
Obligations of manufacturers

Art.14
Reporting obligations of manufacturers

22

A natural or legal person (other than the manufacturer, the importer or the distributor) is **considered to be a manufacturer,** where it carries out a **substantial modification** of a PDEs and makes that product **available on the market.**

That person shall be **subject to the obligations set out in Arts. 13 and 14**
- for the **part of the PDEs that is affected by the substantial modification or,**
- if the substantial modification has an **impact on the cybersecurity** of the PDEs **as a whole, for the entire product**.

Arts. **3,21,22,23**

Products in scope and products out of scope - Table 1

2.1

This Regulation applies to products with digital elements (PDEs) made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

This Regulation does not apply to the following PDEs, as they are already covered by existing sectoral legislation ensuring a level of cybersecurity protection at least equivalent to the one afforded by the CRA:

Key term: **making available on the market**

2.2,3,4,5,6 and 7

Excluded product category	Relevant legal act
2(a) **Medical devices**	**Regulation (EU) 2017/745** (Medical Devices Regulation)
2(b) **In vitro diagnostic medical devices**	**Regulation (EU) 2017/746** (In Vitro Diagnostic Medical Devices Regulation)
2(c) **Motor vehicles, systems, and components**	**Regulation (EU) 2019/2144** (Vehicle Type-Approval and General Safety Regulation)
3 **Products certified under aviation safety rules**	**Regulation (EU) 2018/1139** (Civil Aviation Safety Regulation)
4 **Marine equipment**	**Directive 2014/90/EU** (Marine Equipment Directive)
5 **PDEs covered by other Union rules**	If those rules already set cybersecurity requirements that **address all or part of the same risks** as those covered by the CRA in **Annex I**, and if that legislation **ensures an equal or higher level of protection**, the application of the CRA may be **limited or excluded** for such products.

The European Commission has the power to adopt delegated acts to specify:

- whether such limitation or exclusion is necessary;
- the products and rules concerned; as well as
- the scope of the limitation, if relevant.

6 **Spare parts** that are made available on the market to **replace identical components in PDEs** and that are **manufactured according to the same specifications as the components that they are intended to replace.**

7 **Products** developed or modified exclusively **for national security or defence purposes**, or **specifically designed to process classified information.**

Products within the scope and products out of scope - Table 2

2.1

This Regulation applies to products with digital elements (PDEs) made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

⇨ In addition, this Regulation does not apply to:

Key term: **making available on the market**

3; recital 18

recital 12

Excluded product category	Relevant CRA provisions
8 Non-monetised Free and Open-Source Software (FOSS)	**Recital 18 CRA:** only Free and Open-Source Software (FOSS) made available on the market, and therefore **supplied for distribution or use in the course of a commercial activity**, should fall within the scope of this Regulation. [...] FOSS that **are not monetised** by their manufacturers should not be considered to be a commercial activity. **Art. 3(14) CRA:** **'open-Source Software steward'** means **a legal person, other than a manufacturer**, that has the purpose or objective of systematically **providing support** on a sustained basis for the development of specific PDEs, **qualifying as FOSS** and intended for **commercial activities**, and that ensures the viability of those products. **Art. 3(22) CRA:** **'making available on the market' means the supply of a PDEs for distribution or use on the Union market in the course of a commercial activity**, whether in return for payment or free of charge.
9 Services	**Recital 12 CRA:** as the **Directive (EU) 2022/2555 (NIS2) already applies** to cloud computing services and cloud service models such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). ↳ **Eg.** websites that do not support the functionality of a PDE; cloud services designed and developed outside the responsibility of a manufacturer of a PDE.

Key term: **Free and open-source software**

2.1

This Regulation applies to products with digital elements (PDEs) made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

3.1

'Product with digital elements' means a **software or hardware** product and **its remote data processing solutions**, including software or hardware components being placed on the market separately.

Key term: **Software**

Key term: **Hardware**

Hardware:
- smartphones,
- laptops,
- "smart appliances" (e.g., smart speakers),
- network equipment (e.g., routers),
- CPUs,
- more foundational components,
- consumer devices,
- complex devices,
- etc.

Software, including so-called **non-embedded software**:
- operating systems,
- computer games,
- word processing,
- mobile apps,
- anti-virus,
- software libraries,
- password managers,
- a program that can be downloaded via a website,
- firmware or software meant to be embedded into hardware devices,
- etc.

3.2

'Remote data processing' means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions.

Recital **11**

'This approach ensures that PDEs are secured in their entirety, irrespective of whether data is **processed** or **stored locally** on the user's device or **remotely** by the manufacturer, in so far as processing or storage at a distance is **necessary for a PDE to perform its functions**.

- **Eg.** a mobile application requires access to an application programming interface or to a database provided by means of a service developed by the manufacturer. In such a case, the service falls within the scope of this Regulation as a remote data processing solution (recital 11);
- **Eg.** cloud-enabled functionalities provided by a manufacturer of smart home devices that enable users to control the device at a distance fall within the scope of the CRA (recital 12);
- **Eg.** websites that do not support the functionality of a PDE, or cloud services designed and developed outside the responsibility of a manufacturer of a PDE do not fall within the scope of the CRA (recital 12).

26.2(a)

The Commission will publish **guidance to facilitate CRA's implementation**, in particular, with regard to the notion of remote data processing solutions.

4

Member States **shall not impede**, for the matters covered by this Regulation, **the making available on the market of PDEs** which comply with this Regulation.

At trade fairs, exhibitions, demonstrations or similar events, Member States shall not prevent the presentation or use of a PDEs which does not comply with this Regulation, including its prototypes, provided that

- **the product is presented with a visible sign clearly indicating that it does not comply with this Regulation and that it is not to be made available on the market until it does so.**

Member States shall not prevent the making available on the market of unfinished software which does not comply with this Regulation, provided that

- **the software is made available only for a limited period required for testing purposes;**
- **with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing.**

→ **If a product is considered a safety component** under Union harmonisation legislation other than this Regulation, **the exception** allowing the distribution of unfinished software for testing purposes **does not apply**.

5

This Regulation shall not prevent Member States from subjecting PDEs to additional cybersecurity requirements for the procurement or use of those products for specific purposes, including where those products are procured or used for national security or defence purposes, **provided that**

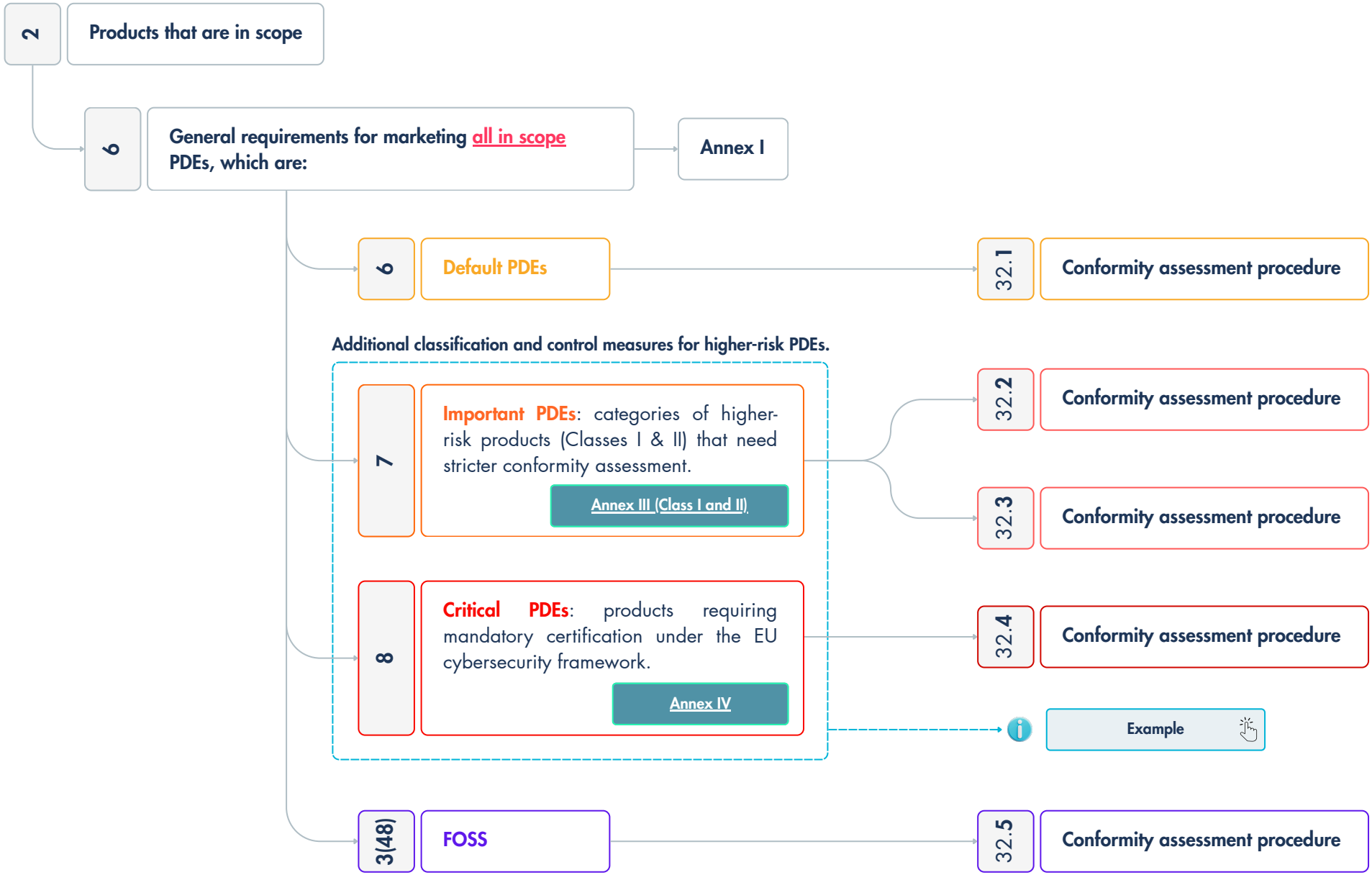
- **such requirements are consistent with Member States' obligations laid down in Union law, and**
- **that they are necessary and proportionate for the achievement of those purposes.**

When PDEs falling within the scope of this Regulation are procured, Member States must take into account whether those products comply with:

- **the essential cybersecurity requirements** set out in Annex I,
- including the manufacturer's **ability to handle vulnerabilities effectively**.

This assessment must form part of the procurement process, **without affecting the application of Directives 2014/24/EU and 2014/25/EU.**

Classificiation of products and corresponding conformity procedure



Essential cybersecurity Requirements (ECR) for PDEs

6

PDEs shall be made available on the market only where:

(a) they meet the essential cybersecurity requirements set out in Part I of Annex I, **provided that**

- they are properly installed, maintained, used **for their intended purpose or under conditions which can reasonably be foreseen**, **and**,
- where applicable, the necessary security updates have been installed; **and**

(b) the processes put in place by the manufacturer **comply with the essential cybersecurity requirements** set out in Part II of Annex I, ensuring continuous security management throughout the product lifecycle.

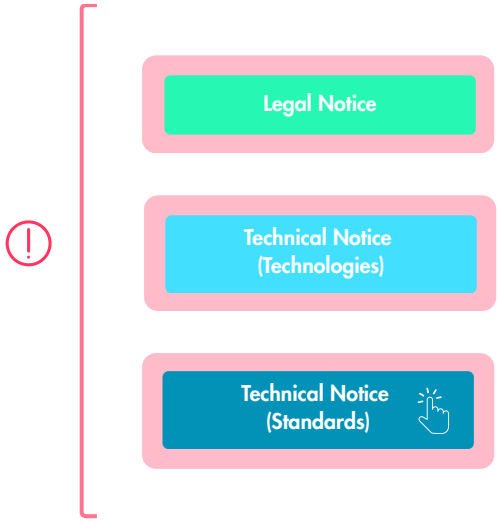
Annex I, part 1

Annex I, part 2

The CRA defines what must be achieved - secure design, development, and maintenance - **but not how to achieve it.**
To bridge this gap, our framework connects each CRA obligation with:

1) **Activities & principles** – the main security practices required by the Regulation (e.g. risk assessment, threat modelling, secure development);
2) **Technologies & tools** – operational instruments that help implement these practices (for example, STRIDE Threat Modelling or OWASP Threat Dragon);
3) **Standards & best practices** – internationally recognised references such as ISO/IEC 27002, ISA/IEC 62443-4-2, and ETSI EN 303 645, which provide structure and assurance.

This **three-layered approach** turns the legal text of Art. 6 and Annex I into actionable guidance that can be directly integrated into product development and compliance workflows.



Annex I - Essential cybersecurity requirements

Part I | Part II

point 1 — **PDEs shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.**

point 2 — **On the basis of the risk assessment** referred to in Article 13(2) **and where applicable, PDEs shall:**

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made PDEs, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) 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, and by using other technical means;

(f) 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, and report on corruptions;

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the PDEs (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

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

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

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

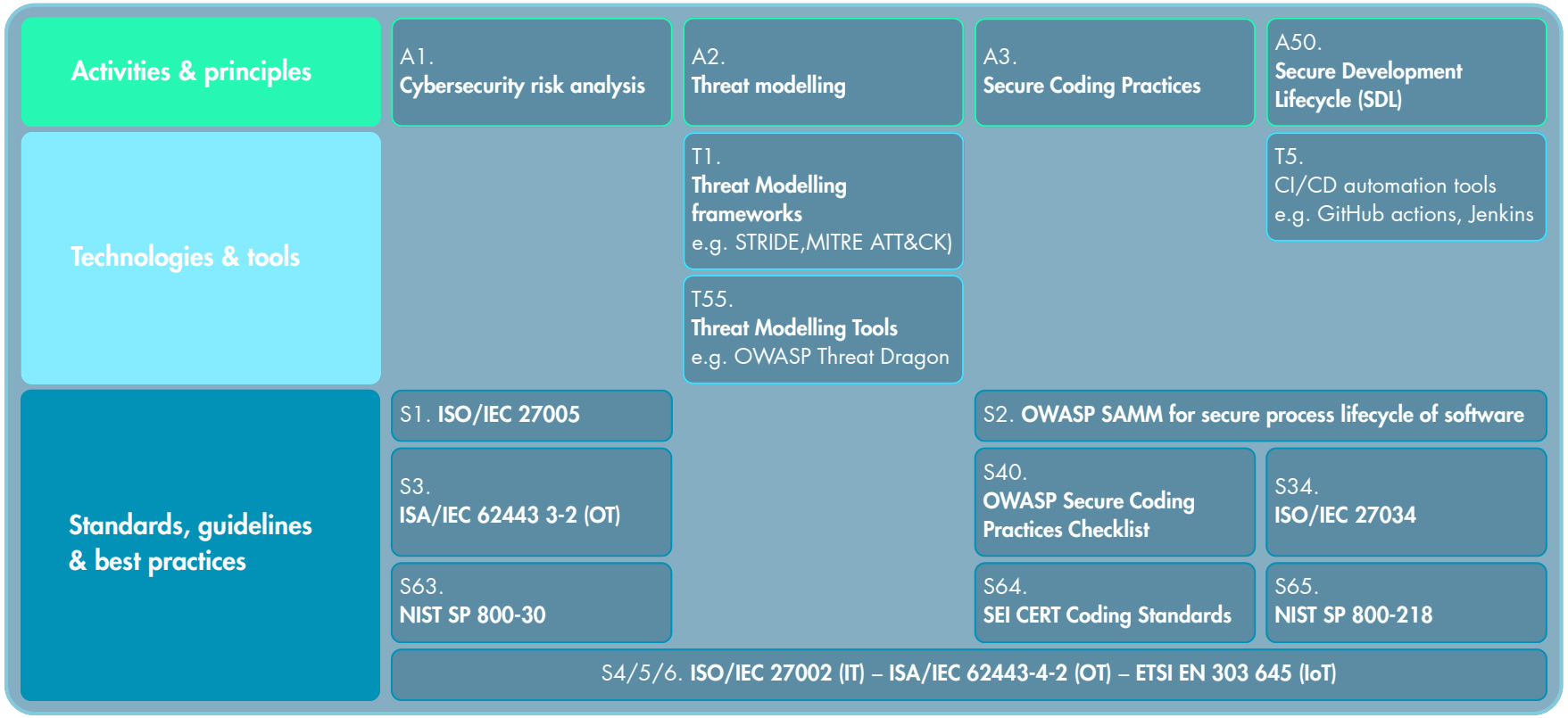
Risk Analysis and secure development

Annex I, **part I, point 1**

PDEs shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

Guidance: ENISA sub requirements (not mandatory)

- 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.).



Click inside this box to enable scrolling.

A1:
Cybersecurity Risk Analysis involves identifying, assessing, and prioritizing potential threats and vulnerabilities that could impact an organization's digital assets or systems. It evaluates the likelihood and impact of cyber incidents to determine risk exposure.

A2:
Threat Modelling is the process of systematically identifying and analyzing potential threats, attack paths, and weaknesses in a system's design or architecture. It helps anticipate how adversaries might exploit vulnerabilities.

A3:

Vulnerability scanning and assessment

Annex I, **part I, point 2(a)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(a) be made available on the market without known exploitable vulnerabilities.

Example

Guidance: ENISA sub requirements (not mandatory)

- A vulnerability assessment should be performed against the digital elements of a product;
- Known exploitable vulnerabilities shall be fixed before the release of the product.

Click inside this box to enable scrolling.

A4:
Vulnerability Assessment is the process of scanning and evaluating systems, networks, or applications to identify known security weaknesses. It provides a structured view of vulnerabilities based on their severity and exploitability, helping prioritize remediation efforts.

A5:
Vulnerability Assessment is the process of scanning and evaluating systems, networks, or applications to identify known security weaknesses. It provides a structured view of vulnerabilities based on their severity and exploitability, helping prioritize remediation efforts.

A6:
CI/CD Security Integration embeds security checks and controls into Continuous Integration and Continuous Deployment pipelines. It automates code scanning

Security by Default

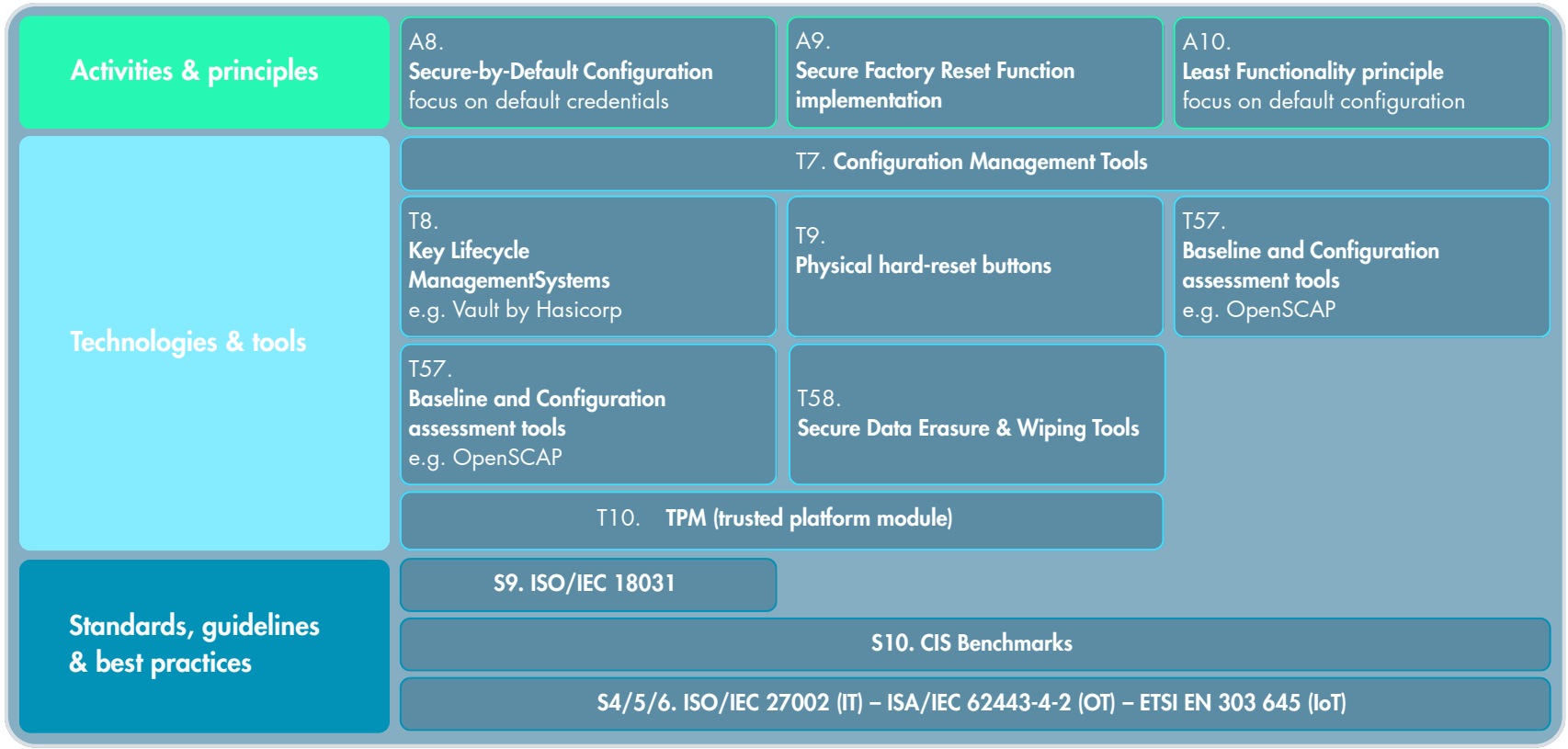
Annex I, **part I, point 2(b)**

On the basis of the risk assessment referred to in Article13.2 **and where applicable, PDEs shall:**

(b) be made available on the market **with a secure by default configuration, unless otherwise agreed between manufacturer and business user** in relation to a tailor-made PDEs, including the **possibility to reset** the product to its original state.

Guidance: ENISA sub requirements (not mandatory)

- In case default configurations foresee an initial/default credential, the same should use a complex and randomly chosen password, different for each product;
- In case default configurations cover cybersecurity items, they should adopt a reasonable level of security for each item;
- The default configuration should be placed in a non-erasable memory;
- A function to reset the product configuration to the default one should be implemented.



Click inside this box to enable scrolling.

A8:
Secure-by-Default Configuration ensures that products and systems are deployed with the most secure settings already enabled, minimizing exposure from the start. It includes enforcing strong authentication policies, disabling unnecessary services, and eliminating default or hardcoded credentials that attackers could exploit.

A9:
Secure Factory Reset Function Implementation ensures that when a device or system is reset, all sensitive data, cryptographic keys, and user configurations are completely erased or securely overwritten. It prevents data recovery after reset and guarantees that the product

Secure update management

Annex I, **part I, point 2(c)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(c) ensure that vulnerabilities can be addressed through security updates, including, **where applicable**, **through automatic security updates** that are installed within an appropriate timeframe enabled as a default setting, **with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.**

Guidance: ENISA sub requirements (not mandatory)

- The company distributing a product or service should provide timely security updates for the software components of the product/service for a reasonable amount of time;
- A function to automatically check the presence of updates and install them, or notify the user of their presence, should be implemented, and where applicable this should be the default initial configuration;
- A product should provide a secure mechanism to install/implement updates;
- The company distributing a product should notify the user on the availability of updates.

Activities & principles	A35. Secure Update management	A36. Secure Update implementation	A37. Automatic Update Checking
Technologies & tools	T40. **Update Frameworks** e.g. Libostree		
	T41. **Code signing with PKI** e.g. X.509 certificates		T42. Alerting mechanism
Standards, guidelines & best practices	S28. **ISO/IEC 30111**		
	S29. **IEC/ISA 62443 2-1 (OT)**		
	S4/5/6. **ISO/IEC 27002 (IT) – ISA/IEC 62443-4-2 (OT) – ETSI EN 303 645 (IoT)**		

Click inside this box to enable scrolling.

A35:
Secure Update Management ensures that software and firmware updates are delivered, verified, and applied in a protected manner, including updates for third-party components. It covers signing, integrity checks, and controlled distribution to prevent tampering, while maintaining up-to-date and secure product ecosystems.

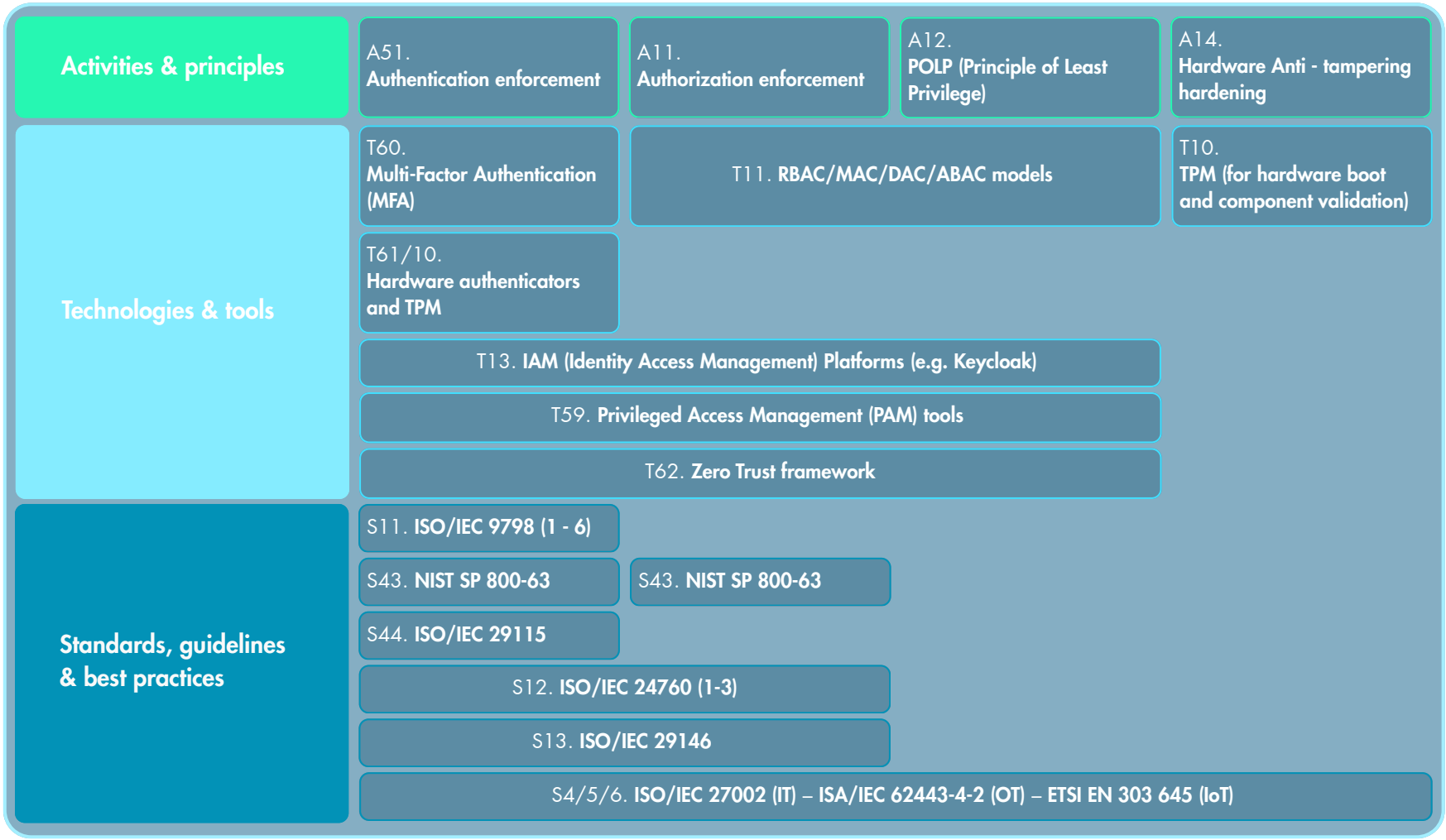
Authentication, authorization and access management

Annex I, **part I, point 2(d)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(d) **ensure protection** from unauthorised access **by appropriate control mechanisms**, including **but not limited to** **authentication, identity or access management systems,** **and report** on possible **unauthorised access**.

Guidance: ENISA sub requirements (not mandatory)

- An appropriate authentication and authorisation system shall be implemented according to the product nature and identified risks;
- The access to personal/protected data and to administration/configuration functions should be granted only to authenticated and authorised users;
- In accordance with the nature of the product and to the relevant risks identified in the risk analysis, physical unauthorized access should be forbidden.



Click inside this box to enable scrolling.

A51:
Authentication Enforcement ensures that only verified users, devices, or processes can access a system or application. It requires strong and consistent authentication mechanisms such as multi-factor authentication, credential protection, and session validation to prevent impersonation or unauthorized access.

A11:
Authorization Enforcement ensures that users, devices, and processes can only access resources and perform actions consistent with their assigned permissions. It relies on well-defined access control policies and mechanisms that validate every request after authentication, preventing privilege escalation or

Data confidentiality

Annex I, **part I, point 2(e)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(e) **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, and by using other technical means.

Guidance: ENISA sub requirements (not mandatory)

- Data stored in a product's internal memory should be encrypted at rest using current non-deprecated technology;
- Transmission protocols used to send/receive data should support encrypted communications and enable them by default;
- The product should implement symmetric or asymmetric encryption schemes (including PKIs) deprecated technology to ensure that confidentiality of exchanged data is protected.

Activities & principles	A15. **Data encryption at rest**	A16. **Data encryption in transit**	A17. **Key management and rotation**
Technologies & tools	T14. **Data encryption algorithms** (e.g. AES 256) **and libraries** (e.g. OpenSSL)		T15. **Public Key Infrastructures for keys certification**
	T63. **Storage-level encryption** e.g. LUKS, BitLocker	T16. **Secure communication protocols (Transport and Application layer)** [TLS, HTTPS]	T8. **Key Lifecycle Management Systems** e.g. Vault by Hashicorp
	T64. **Filesystem-level encryption** e.g. fscrypt	T66. **Network Layer Encryption (VPN & IPsec)**	T10. **TPM (focus on key storage)**
	T65. **Database encryption (TDE and field level)**		
Standards, guidelines & best practices	S47. **NIST SP 800-111**	S48. **NIST SP 800-77**	S49. **NIST SP 800-57**
	S14. **ISO/IEC 18033 (1-7)**		
	S15. **OWASP Cryptographic Storage Guidelines**	S16. **ITU-T X.805**	S9. **ISO/IEC 18031**
	S4/5/6. **ISO/IEC 27002 (IT) – ISA/IEC 62443-4-2 (OT) – ETSI EN 303 645 (IoT)**		

Click inside this box to enable scrolling.

A15:
Data Encryption at Rest protects stored information by encrypting it when saved on physical media such as disks, SSDs, or databases. It relies on cryptographic protocols and algorithms such as AES, RSA, or elliptic curve cryptography to ensure that data remains unreadable without valid decryption keys.

A16:
Data Encryption in Transit protects information as it moves across networks or communication channels between systems, devices, or users. It uses secure cryptographic protocols such as TLS, SSH, or IPsec to ensure confidentiality, integrity, and authentication during data transmission.

Data and system Integrity

Annex I, **part I, point 2(f)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(f) 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, **and report on corruptions**.

Guidance: ENISA sub requirements (not mandatory)

- Integrity of data, programs and configurations stored in the product's internal memory should be ensured using current non-deprecated technology, e.g. hashing;
- Transmission protocols used to send/receive data should support ways to ensure it is possible to spot data alteration during the transmission (e.g. MACs);
- The product should implement symmetric or asymmetric encryption schemes (including public key infrastructures) to ensure that the integrity of exchanged data is protected;
- A product should perform self-test to verify integrity of relevant code/information (e.g. firmware).

Activities & principles	A18. **Hashing and message validation**	A19. **Self-integrity control**	A15/A16. **Data encryption at rest and in transit**	A17. **Key management and rotation**
Technologies & tools	T18. **Cryptographic Hash Algorithms and Libraries** e.g. SHA-256, OpenSSL	T19. **File and System Integrity Monitoring tools** e.g. AIDE, Wazuh)	T14. **Data encryption algorithms** with integrity enforcement via AEAD or MAC	T15. Public key Infrastructures
	T20. **Message Authentication Codes** e.g. MACs/HMACs		T16/66. **Secure communication protocols (with digital hashing)** e.g. IPsec con ESP/AH	T8. **Key Lifecycle Management Systems** e.g. Vault by Hashicorp
Standards, guidelines & best practices	S45. **ISO/IEC 10118**			S49. **NIST SP 800-57**
	S17. **ISO/IEC 9796**		S14. **ISO/IEC 18033 (1-7)**	S9. **ISO/IEC 18031**
	S18. **ISO/IEC 9797**			
	S4/5/6. **ISO/IEC 27002 (IT) – ISA/IEC 62443-4-2 (OT) – ETSI EN 303 645 (IoT)**			

Click inside this box to enable scrolling.

A18:
Hashing and Message Validation ensure data integrity by generating fixed-length hashes that uniquely represent original content. They enable detection of unauthorized modifications and support message authentication when combined with cryptographic mechanisms like HMAC or digital signatures.

A19:
Self-Integrity Control allows a system or component to verify its own integrity during startup or runtime by checking code, configuration, or firmware against trusted references. It detects unauthorized modifications or tampering and

Data minimisation

Annex I, **part I, point 2(g)**

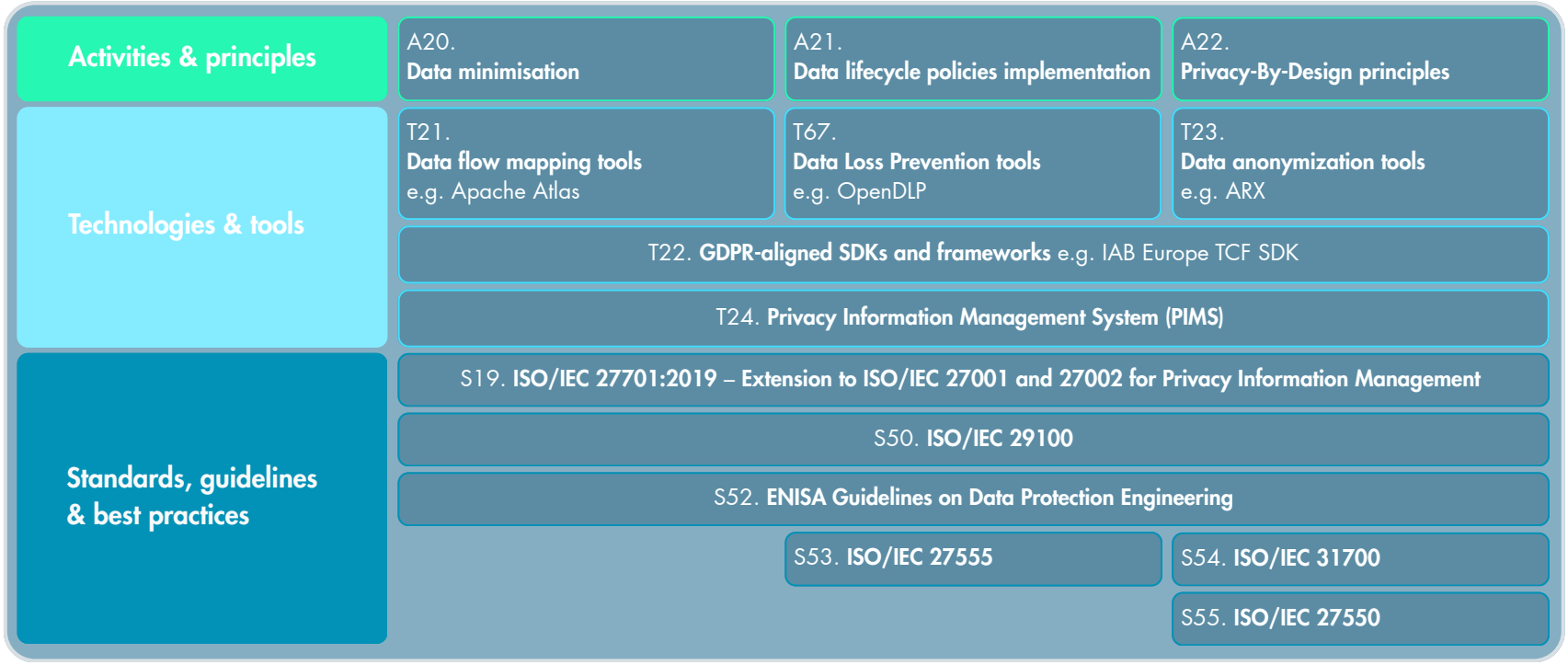
On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(g) **process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose** of the PDEs (data minimisation).

Guidance: ENISA sub requirements (not mandatory)

In general, refer to GDPR best practices, such as:

- it should not be asked to the user the provision of data that is not strictly necessary to the execution of the task or service requested;
- data no longer needed should be deleted without delay.



Click inside this box to enable scrolling.

A20:
Data Minimisation limits the collection, storage, and processing of personal or operational data to only what is strictly necessary for a specific purpose. It reduces exposure in case of breaches and supports compliance with privacy and security principles by minimizing unnecessary information.

A21:
Data Lifecycle Policies Implementation establishes rules for how data is created, classified, stored, retained, and securely deleted throughout its lifespan. It ensures consistent handling of information, reduces unnecessary

Availability and Resilience

Annex I, **part I, point 2(h)**

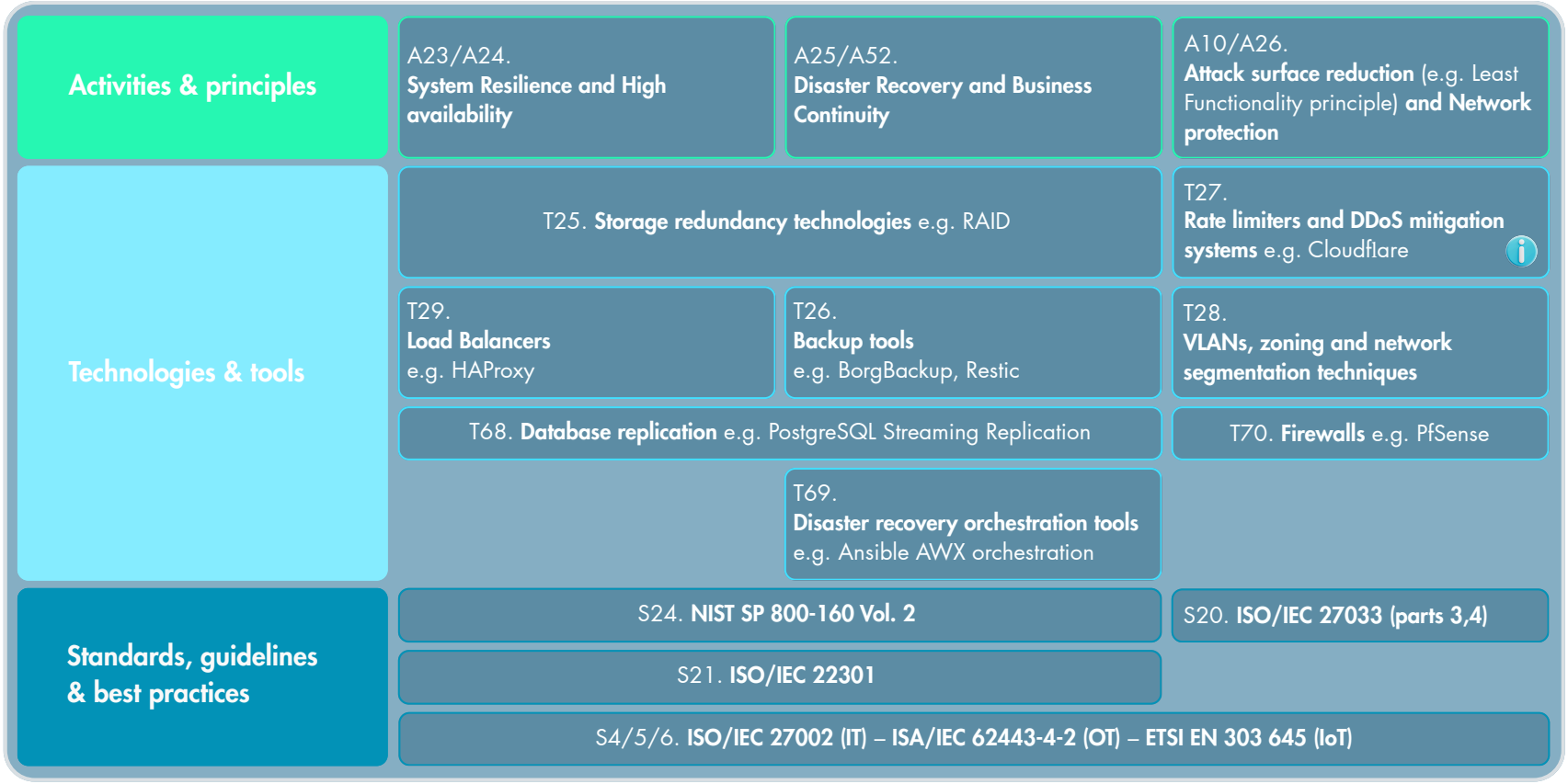
On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(h) **protect the availability of essential and basic functions**, **also after an incident**, including through resilience and mitigation measures against denial-of-service attacks.

Guidance: ENISA sub requirements (not mandatory)

The product should be hardened against attacks, like for instance distributed denial of service attacks, by implementing, among other things, the following measures if appropriate:

- reverse proxies network segmentation;
- load balancing;
- rate limiting;
- redundancy and high availability solutions;
- backup sites;
- disaster recovery plans;
- minimize offered services.



Click inside this box to enable scrolling.

A23:
Log Rotation and Retention manage how logs are stored, archived, and periodically cycled to prevent excessive storage use and preserve essential records. They ensure that older logs are securely archived or deleted according to policy while keeping recent logs accessible for monitoring, auditing, and investigations.

A24:
High Availability (strictly related to system resilience) ensures that systems and services remain accessible with minimal downtime, even in the event of hardware failures or maintenance activities. It relies on redundancy, failover mechanisms, and load balancing to maintain continuous and reliable

Minimise Impact on External Services

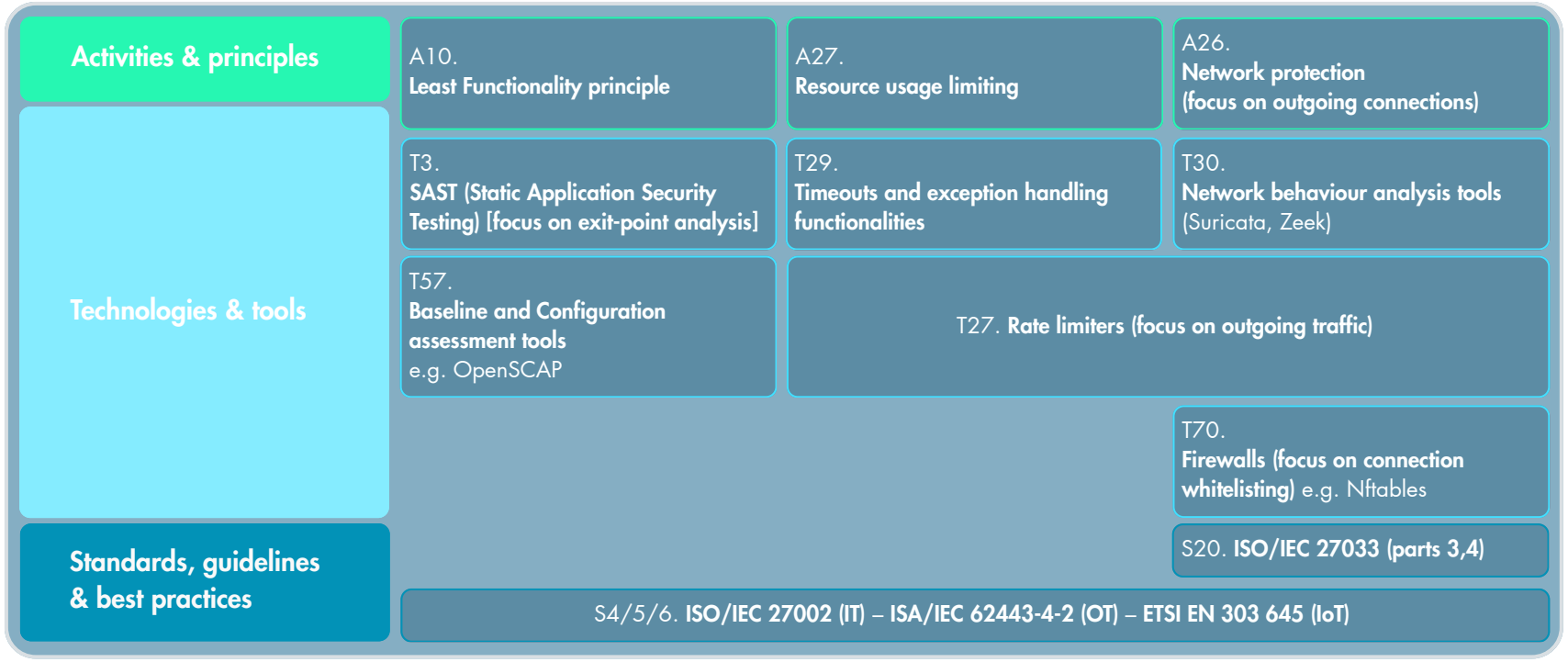
Annex I, **part I, point 2(i)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.

Guidance: ENISA sub requirements (not mandatory)

- The product should limit outgoing network connections to what is strictly needed;
- The product should implement measures such as timeouts and exception handling to avoid generating multiple requests to a busy/not responsive service.



Click inside this box to enable scrolling.

A10:
Least Functionality Principle requires systems to operate with only the features, services, and privileges strictly necessary for their intended purpose. It reduces the attack surface by disabling or removing unused components. Default configurations should reflect this principle, ensuring that nonessential services are turned off and unnecessary interfaces are not exposed by default.

A27:
Resource Usage Limiting restricts how much CPU, memory, storage, or network bandwidth processes or users can consume. It prevents resource exhaustion attacks,

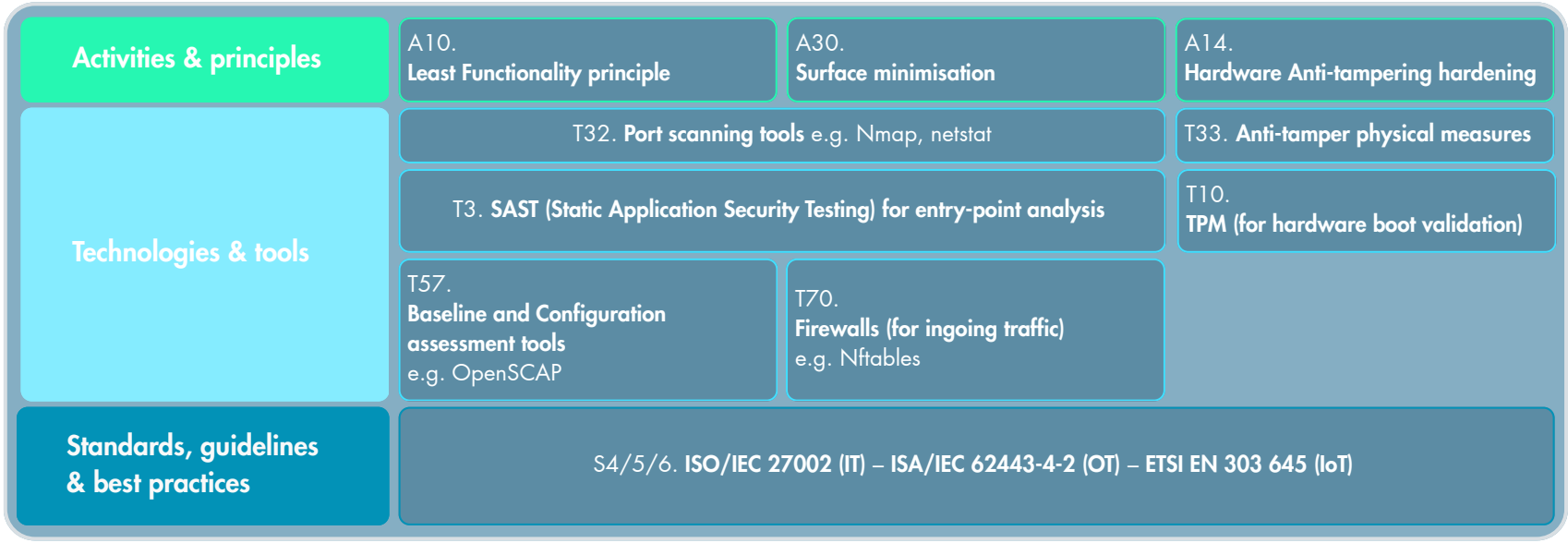
Least Functionality and surface minimisation

Annex I, **part I, point 2(j)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(j) be designed, developed and produced to limit attack surfaces, including external interfaces.

Guidance: ENISA sub requirements (not mandatory)

- The product's hardware design should limit all the connections and interfaces that are not strictly required for performing the various tasks the product is expected to do;
- If required by a risk assessment, a physical product should include tamper-resistant features;
- The product/service should have all not essential network ports closed as a default configuration;
- Software present in digital product should be designed to avoid having unnecessary entry points (e.g. API) open and available for external unauthorised callers.



Click inside this box to enable scrolling.

A10:
Least Functionality Principle requires systems to operate with only the features, services, and privileges strictly necessary for their intended purpose. It reduces the attack surface by disabling or removing unused components. Default configurations should reflect this principle, ensuring that nonessential services are turned off and unnecessary interfaces are not exposed by default.

A30:
Surface Minimisation reduces the

Data and system Integrity

Annex I, **part I, point 2(k)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.

Guidance: ENISA sub requirements (not mandatory)

- The product should be designed in a way that gaining unauthorised access to a function or data does not automatically lead to a complete access to all product's functions and data (defence in depth principles);
- Sensitive data stored in a product's internal memory should be encrypted at rest;
- The product should not store data that is not relevant or necessary to perform its tasks (data minimisation).

Activities & principles

- A31. **Defence-in-Depth principles**
- A32/A12. **Privilege separation and POLP**
- A20. **Data minimisation**
- A15. **Data encryption at rest**

Technologies & tools

- T10/T31. **TPM and Secure boot [for Hardware-level defence layer]**
- T59. **Privileged Access Management (PAM) tools**
- T22. **GDPR-aligned SDKs and frameworks** e.g. IAB Europe TCF SDK
- T63/64/65. **Storage, Filesystem and Database level encryption for data-level defence layer**
- T70. T11. **RBAC/MAC/DAC/ABAC models (for OS-level defence layer)**
- T14. **Data encryption algorithms** (e.g. AES 256) **and libraries** (e.g. OpenSSL)
- T70. **Web ApplicationFirewalls** e.g. Modsecurity **[for application-level defence layer]**
- T72. **Memory Protection and Exploit Mitigations mechanism** e.g. NX, ASLR **[for OS-level defence layer]**
- T63/64/65. **Storage, Filesystem and Database level encryption (for data-level defence layer)**

Click inside this box to enable scrolling.

A31:
Defence-in-Depth Principles apply multiple, layered security controls across systems so that if one layer fails, others still provide protection. This approach combines technical, procedural, and physical safeguards to slow attackers, limit lateral movement, and increase overall security robustness.

A32:
Privilege Separation divides system functions into isolated components, each running with the minimum privileges needed for its specific tasks. It prevents a compromise in one component from granting broad system control and limits the potential impact of

Standards, guidelines & best practices

- S18. **ISO/IEC 9797**
- S50. **ISO/IEC 29100**
- S51. **ISO/IEC 29151**
- S25. **NIST SP 800-53 rev.5 – Security and Privacy Controls**
- S4. **ISO/IEC 27002 (IT)**

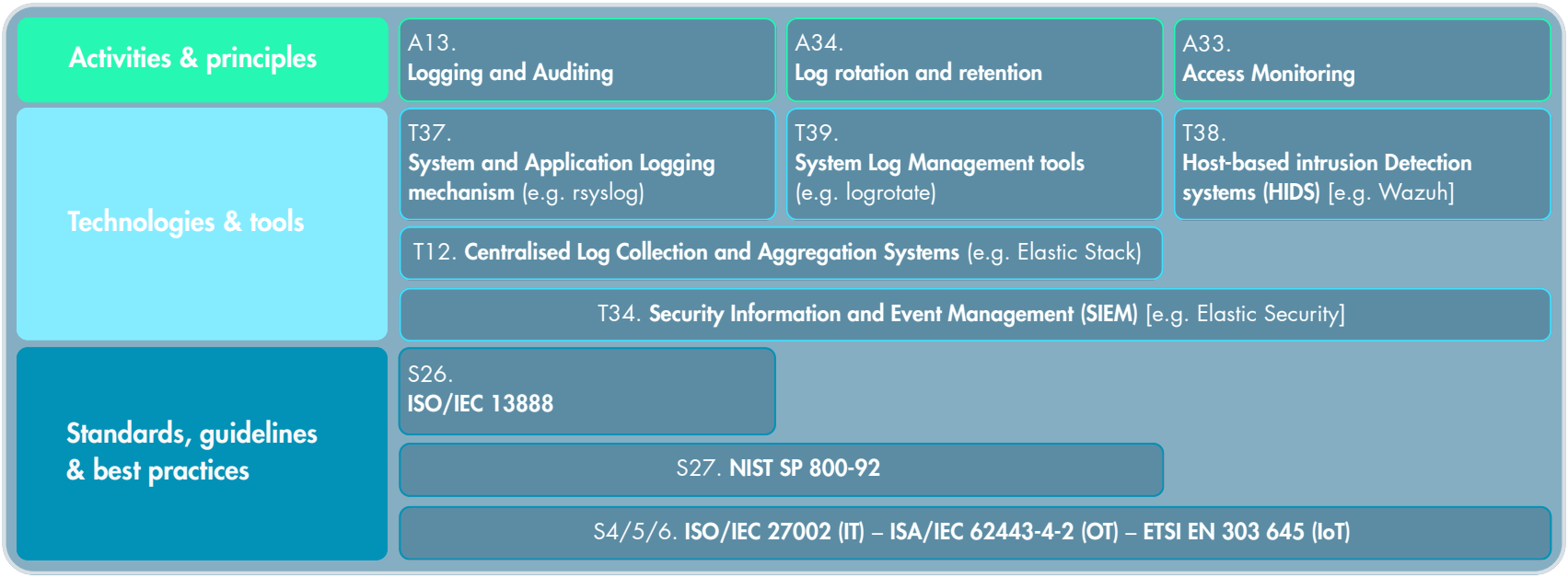
Audit and monitoring

Annex I, **part I, point 2(l)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, **with an opt-out mechanism for the user**.

Guidance: ENISA sub requirements (not mandatory)

- A product should contain a log of cybersecurity related events;
- Access or modification of data, services or functions should be logged;
- Such log should be accessible to the privileged user;
- Logs should be protected from unauthorised modification or corruption.



Click inside this box to enable scrolling.

A13:
Logging and Auditing involve systematically recording security-relevant events and activities across systems, networks, and applications. Logs capture details such as user actions, access attempts, and configuration changes, while auditing verifies their integrity and reviews them for anomalies or signs of compromise.

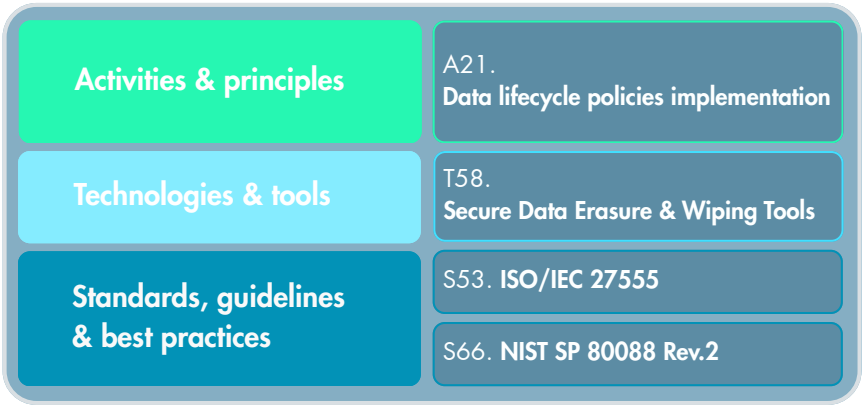
A34:
Log Rotation and Retention manage how logs are stored, archived, and periodically cycled

Secure data deletion

Annex I, **part I, point 2(m)**

On the basis of the risk assessment referred to in Article 13.2 **and where applicable, PDEs shall:**
(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be **transferred** to other products or systems, ensure that this is done **in a secure manner**.

Guidance: ENISA sub requirements (not mandatory)
- data no longer needed should be deleted without delay.



Click inside this box to enable scrolling.

A21:
Data Lifecycle Policies Implementation establishes rules for how data is created, classified, stored, retained, and securely deleted throughout its lifespan. It ensures consistent handling of information, reduces unnecessary retention, and aligns data management with security and compliance requirements.

T58:
Privileged Access Management (PAM) Tools control, monitor, and secure accounts with elevated privileges to reduce the risk of misuse or compromise. They provide credential vaulting, session recording, and just-in-time access to ensure accountability and limit exposure of critical administrative rights.

Manufacturers of the PDE shall:

(1) identify and document vulnerabilities and components contained in PDE, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to PDE, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the PDE;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the PDE affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

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

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their pde as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the PDE;

(7) provide for mechanisms to securely distribute updates for PDE to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made PDE, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Vulnerabilities documentation and SBOM definition

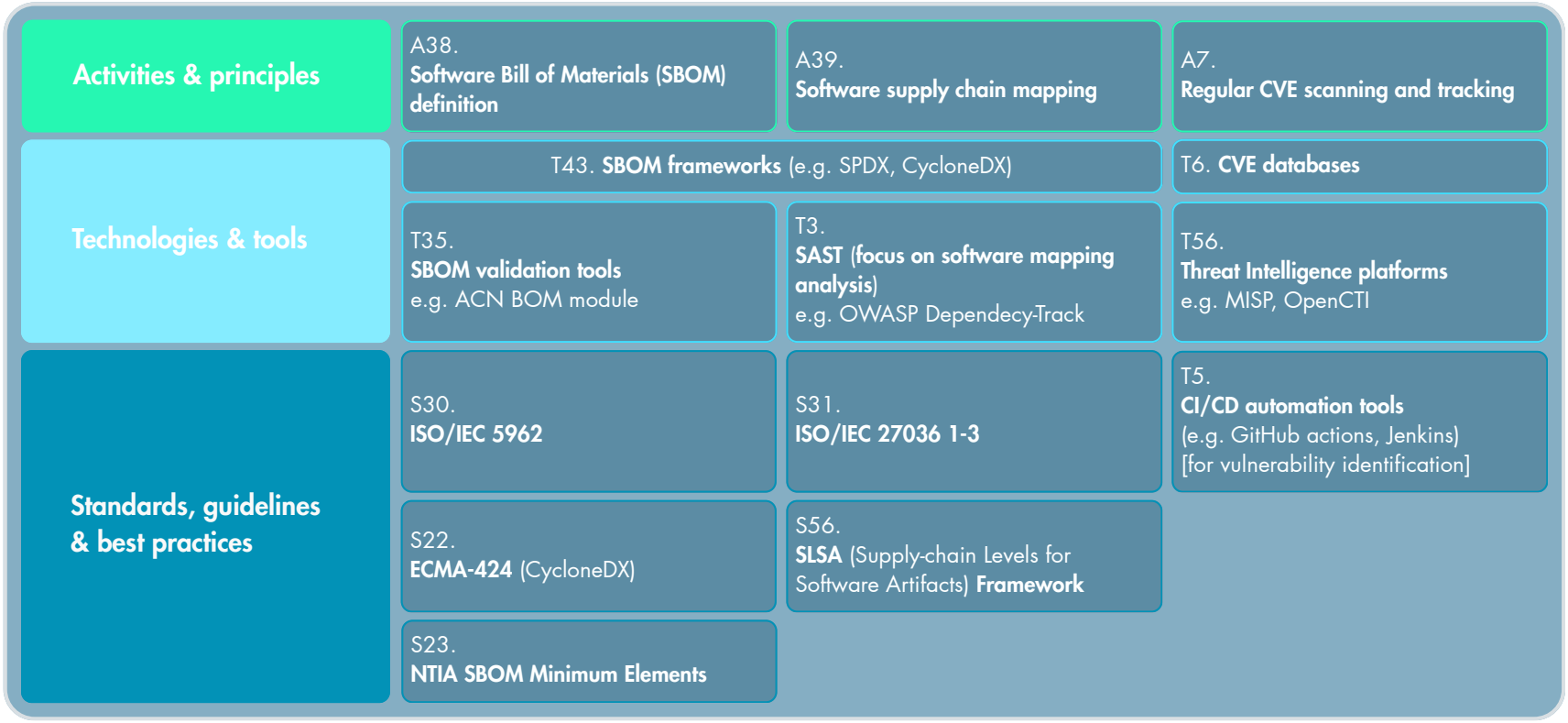
Annex I, **part II**, **point 1**

Manufacturers of the PDE shall:

(1) identify and document vulnerabilities and components contained in PDE, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products.

Guidance: ENISA sub requirements (not mandatory)

- A monitoring of the cybersecurity status of the overall supply chain for the acquisition of the necessary components incorporated in the product should be put in place;
- All libraries and external components used in the software part of a product, including their version number should be listed in a Software Bill of Material (SBOM) available to the user;
- Such Software bill of materials (SBOM) should be compliant to the relevant standards (e.g., ISO/IEC 5921:2021 also known as SPDX [2] or CycloneDX [4] standard).



Click inside this box to enable scrolling.

A38:
Software Bill of Materials (SBOM) Definition involves creating a detailed, machine-readable inventory of all software components, libraries, and dependencies included in a product. It captures versions, origins, and relationships between components to support transparency, vulnerability tracking, and supply-chain security.

A39:
Software Supply Chain Mapping identifies and documents all external components, suppliers, services, and development processes involved in building a product. It visualizes dependencies, data flows, and

Vulnerabilities management and patching

Annex I, **part II**, **point 2**

Manufacturers of the PDE shall:

(2) in relation to the risks posed to PDE, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates.

Guidance: ENISA sub requirements (not mandatory)

- In case vulnerabilities are found they should be classified in accordance with standard severity metrics (e.g. CVSS);
- Vulnerabilities that can be directly fixed by the company should be fixed without delay, in accordance to their severity and the posed risks;
- In case a vulnerability is found in a software component of a product (including libraries and third party components), an update should be prepared and distributed as soon as possible;
- The company developing a product or service should be subscribed to updates coming from CERTs and cybersecurity organisations and analyse them in order to spot vulnerabilities in their products;
- The company developing a product or service should remain updated on the release of new versions of the libraries or third party software components included in their products/services and update the relative software whenever such new version includes a security update.

Activities & principles	A40. **Vulnerability classification and prioritization**	A7. **Regular CVE scanning and tracking**	A35. **Secure Update management** (with a focus also on third-party software)
Technologies & tools	T44. **FIRST CVSS** (Common Vulnerability Scoring System)	T6. **CVE databases**	T40. **Update Frameworks** (e.g. libostree)
	T46. **FIRST EPSS** (Exploit Prediction Scoring System)	T56. **Threat Intelligence platforms** e.g. MISP, OpenCTI	T41. **Code signing with PKI** e.g. X.509 certificates
	T71. **Vulnerability management platforms** (with scoring support) e.g. DefectDojo	T47. **CERT feeds** (e.g. national an international entities)	T45. **Patch and update orchestrator systems** (e.g. Windows Server Update Services*)
		T5. **CI/CD automation tools** e.g. GitHub actions, Jenkins	
Standards, guidelines & best practices		S32. **ISO/IEC 29147**	S28. **ISO/IEC 30111**
	S4. **ISO/IEC 27002 (IT)**		

Click inside this box to enable scrolling.

A40:
Vulnerability Classification and Prioritization evaluates discovered vulnerabilities by categorizing them based on type, severity, and potential impact. It uses metrics such as CVSS or EPSS to rank issues, helping determine which weaknesses require immediate remediation and which can be addressed later based on risk.

A7:
Regular CVE Scanning and Tracking involves continuously monitoring public vulnerability databases, security advisories, and threat intelligence feeds to identify newly disclosed CVEs affecting software or components in use. It enables early awareness of emerging risks and supports

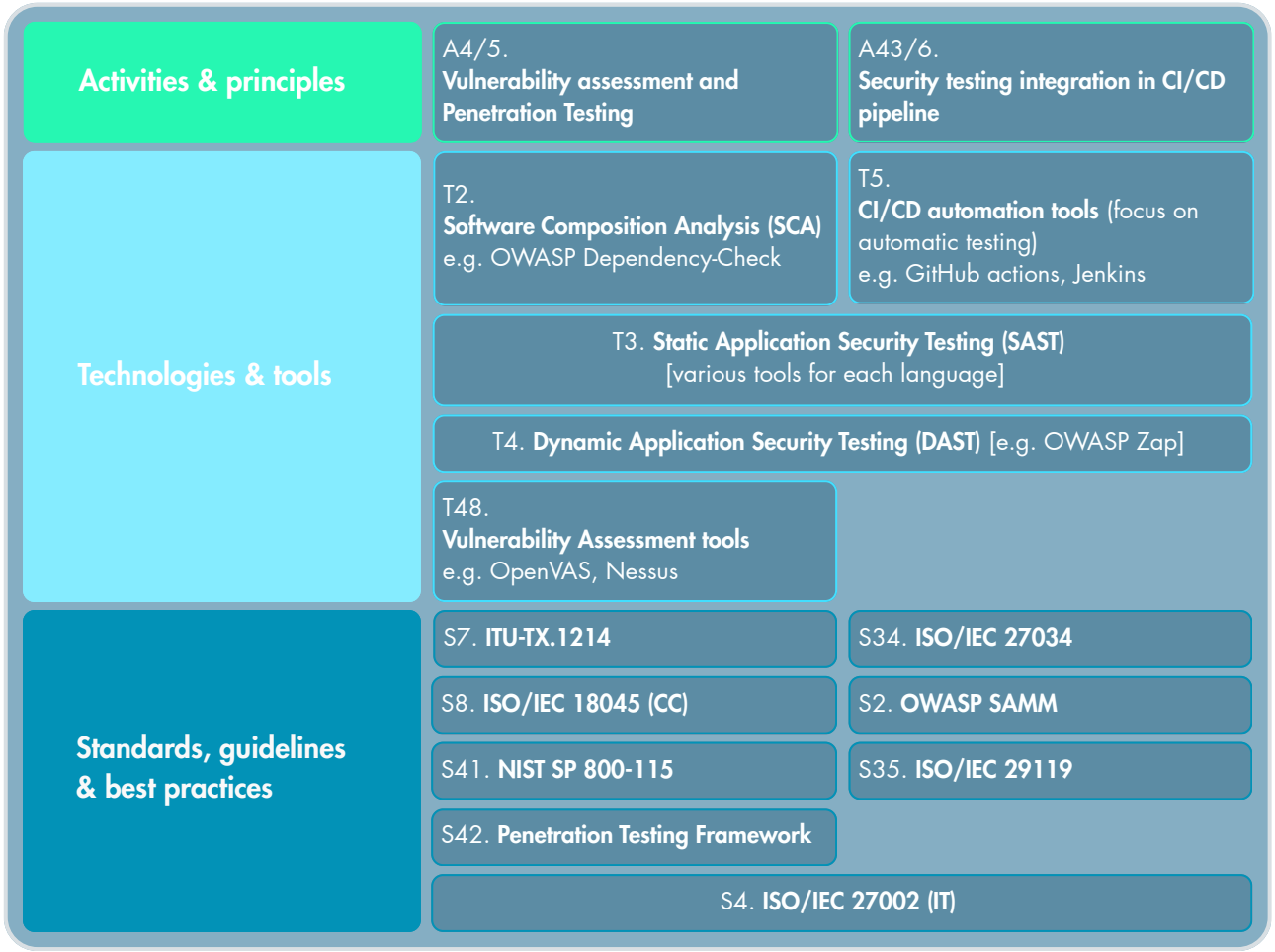
Security testing and assessment

Annex I, **part II**, **point 3**

Manufacturers of the PDE shall:
(3) apply effective and regular tests and reviews of the security of the PDE.

Guidance: ENISA sub requirements (not mandatory)

- Periodic vulnerability assessment should be executed, especially towards those components that present the highest risk;
- When developing or maintaining software components, automatic tests should be executed whenever a new commit/build/version is prepared, if possible, using Continuous Integration/Continuous Deployment (CI/CD) techniques;
- A risk assessment should be re-evaluated whenever there is a significant change in one of the dimensions analysed (new threats, new vulnerabilities, etc.) or a new product release.



Click inside this box to enable scrolling.

A4:
Vulnerability Assessment is the process of scanning and evaluating systems, networks, or applications to identify known security weaknesses. It provides a structured view of vulnerabilities based on their severity and exploitability, helping prioritize remediation efforts.

A5:
Vulnerability Assessment is the process of scanning and evaluating systems, networks, or applications to identify known security weaknesses. It provides a structured view of vulnerabilities based on their severity and exploitability, helping prioritize remediation efforts.

A43:
Security Testing Integration embeds automated security checks directly into CI/CD pipelines. It ensures that vulnerabilities are detected during each build or deployment stage, enabling continuous validation of code security and reducing the risk of introducing flawed components into production.

A6:
CI/CD Security Integration embeds security checks and controls into Continuous Integration and Continuous Deployment pipelines. It automates code scanning, dependency analysis, and configuration validation at every

Public disclosure of fixed vulnerabilities and security advisory management

Annex I, **part II**, **point 4**

Manufacturers of the PDE shall:

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the PDE affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.

Guidance: ENISA sub requirements (not mandatory)

- New CVE indicators should be publicly released and disseminated as soon as the relative security update has been released or implemented.

Click inside this box to enable scrolling.

A28:
Security Advisory and Vulnerability Disclosure Management involves receiving, analyzing, and tracking reported vulnerabilities, then communicating fixes or mitigations through clear security advisories. It ensures coordinated handling with researchers, users, and authorities, and maintains transparent, timely disclosure practices for identified issues.

T49:
Vulnerability Disclosure Platforms provide structured environments for submitting, tracking, and coordinating vulnerability reports between researchers, vendors, and authorities. Solutions like CERT platforms centralize intake, automate communication workflows, and support the secure exchange of technical details to enable responsible and timely disclosure.

T54:
Threat Modelling Tools assist in visualizing system architectures, identifying attack surfaces, and documenting potential threats. Solutions like OWASP Threat Dragon automate diagram creation, apply frameworks such as STRIDE, and generate threat reports to support secure design and risk mitigation.

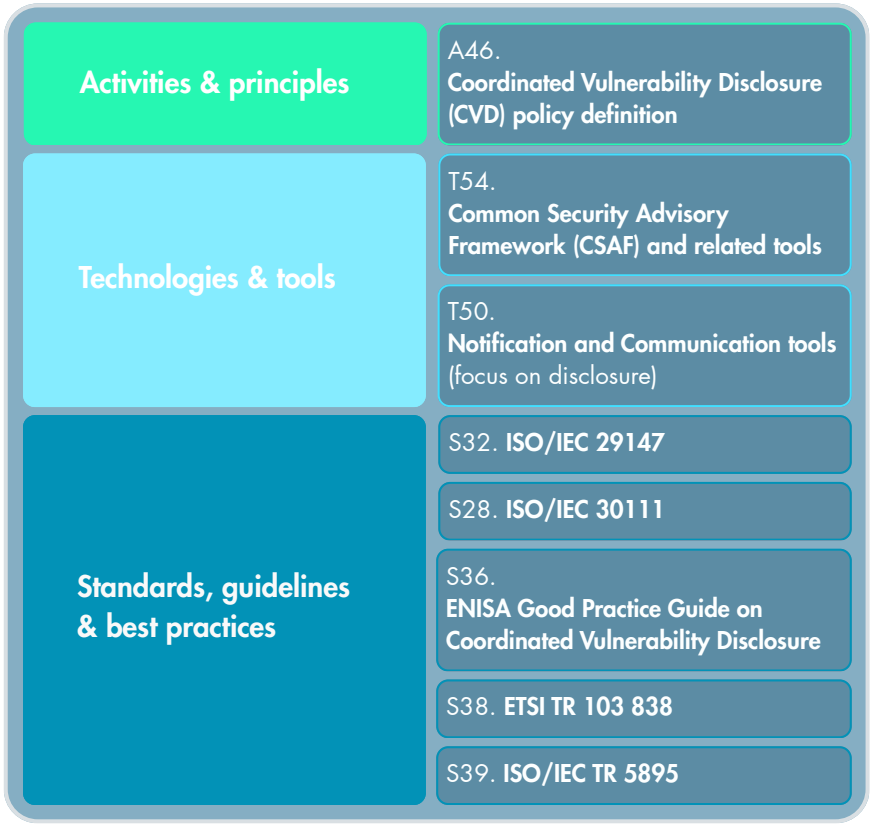
T50:

Coordinated vulnerability disclosure

Annex I, **part II**, **point 5**

Manufacturers of the PDE shall:
(5) put in place and enforce a policy on coordinated vulnerability disclosure.

Guidance: ENISA sub requirements (not mandatory)
- The company should adopt and enforce the CVD policy.



Click inside this box to enable scrolling.

A46:
Coordinated Vulnerability Disclosure (CVD) Policy Definition establishes formal rules and procedures for how vulnerabilities are reported, validated, and disclosed in collaboration with researchers and stakeholders. It defines timelines, communication channels, and coordination practices to ensure transparent and responsible handling of security issues.

T54:
Threat Modelling Tools assist in visualizing system architectures, identifying attack surfaces, and documenting potential threats. Solutions like OWASP Threat Dragon automate diagram creation, apply frameworks such as STRIDE, and generate threat reports to support secure design and risk mitigation.

T50:
Notification and Communication Tools provide secure and reliable channels for submitting and sharing vulnerability information and update notices. Mechanisms like RFC 9116 security.txt, encrypted email, and authenticated mailing systems ensure confidentiality and integrity, while standard communication channels support broad and accessible outreach when security updates or advisories are published.

S32:
ISO/IEC 29147 provides guidelines for vulnerability disclosure, defining how organizations should receive, assess, and publish information about security vulnerabilities in their

Vulnerability information sharing

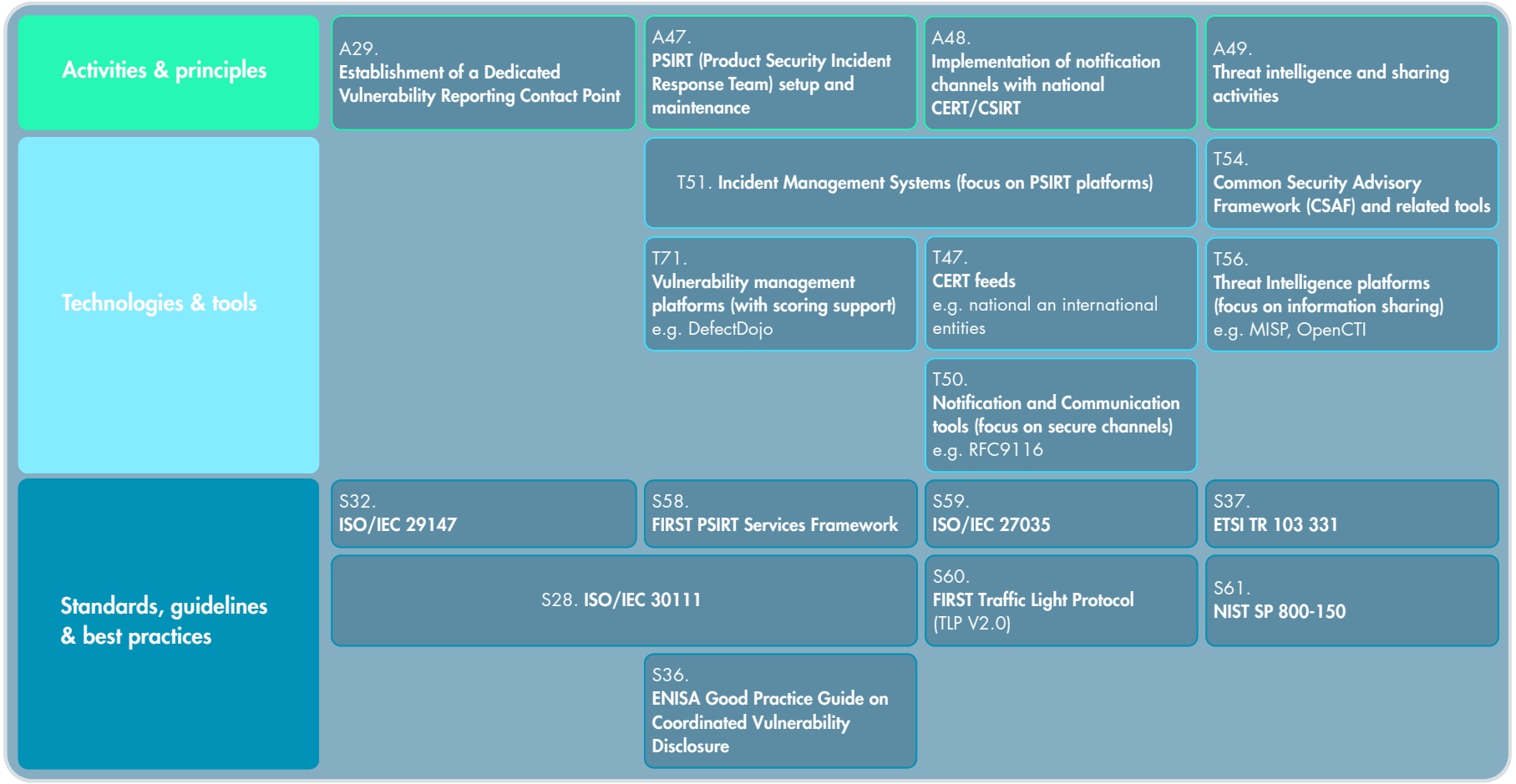
Annex I, **part II**, **point 6**

Manufacturers of the PDE shall:

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their pde as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the PDE.

Guidance: ENISA sub requirements (not mandatory)

- The company distributing a product/service should have a contact point specifically advertised to collect information related to vulnerabilities found in their products/services. If the company has one, this contact point should be the company's PSIRT;
- The company distributing a product/service should inform any relevant authority (e.g. national CERT/CSIRT) about how they can be reached in a timely manner for reasons related to the handling of vulnerabilities.



Click inside this box to enable scrolling.

A29:
Establishment of a Dedicated Vulnerability Reporting Contact Point creates an official, easily accessible channel for submitting vulnerability reports, such as a security mailbox or security.txt entry. It ensures secure communication, authenticated intake, and proper routing of reports to the responsible security team for analysis.

A47:
PSIRT (Product Security Incident Response Team) Setup and Maintenance establishes a dedicated team responsible for receiving, analyzing, and managing product-related vulnerabilities. It defines

Secure update distribution

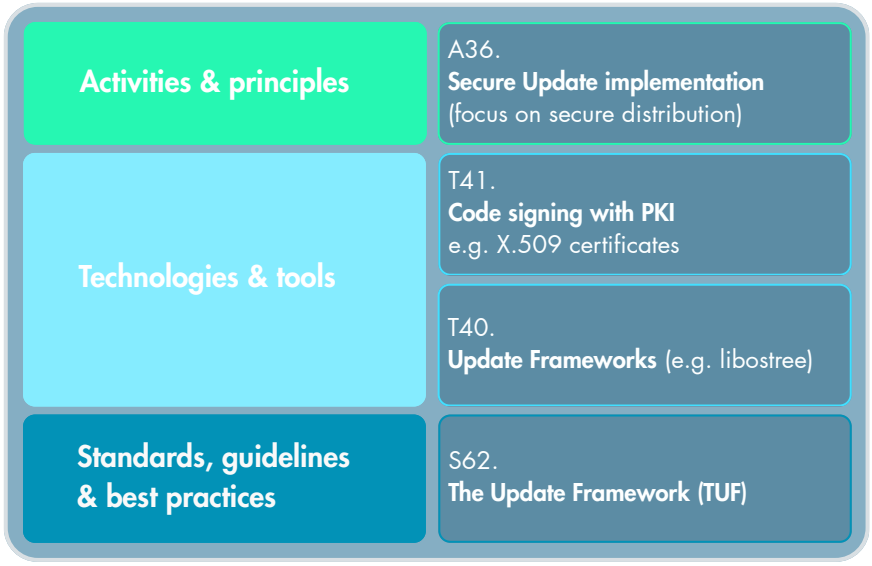
Annex I, **part II**, **point 7**

Manufacturers of the PDE shall:

(7) provide for mechanisms to securely distribute updates for PDE to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.

Guidance: ENISA sub requirements (not mandatory)

- Security updates should be digitally signed using a Code Signing Certificate to ensure the identity of the issuer;
- Hashes of the updates should be made publicly available with instructions on how to verify them.



Click inside this box to enable scrolling.

A36:
Secure Update Implementation focuses on preparing and packaging software or firmware updates with proper signing and integrity protections, including secure distribution mechanisms. It ensures that updates are authenticated, tamper-resistant, and delivered through trusted channels so that only verified code is installed on devices or systems.

T41:
Code Signing with PKI uses cryptographic certificates, such as X.509, to verify the authenticity and integrity of software before installation or execution. Developers sign code with private keys, and systems validate signatures using trusted public keys, ensuring that only legitimate and untampered software is accepted.

T40:
Update Frameworks provide structured mechanisms for packaging, delivering, and verifying software or firmware updates with integrity and authenticity guarantees. Solutions like libostree use content-addressed storage, atomic upgrades, and cryptographic verification to ensure reliable, tamper-resistant update processes across devices and systems.

S62:
The Update Framework (TUF) is a security framework designed to protect software update systems from attacks such

Timely and proper distribution of security updates

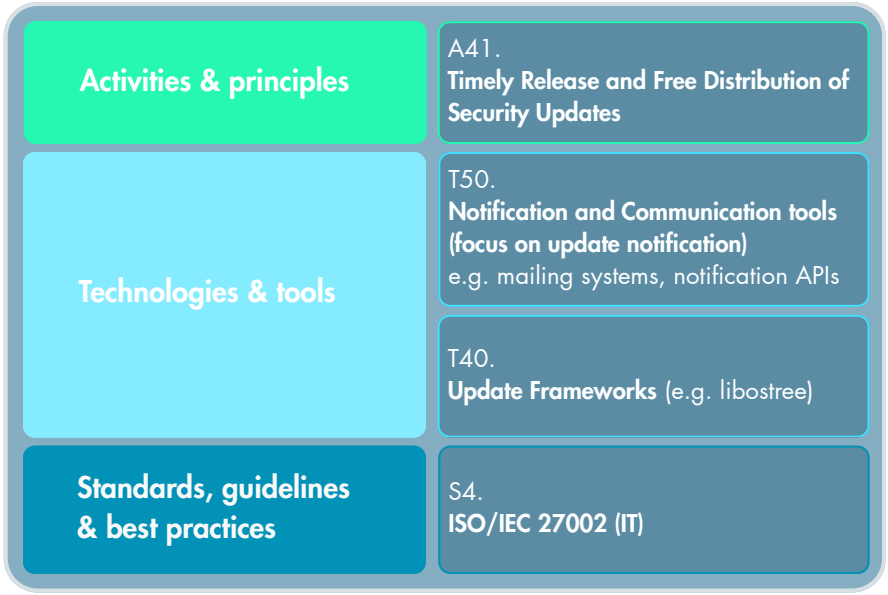
Annex I, **part II**, **point 8**

Manufacturers of the PDE shall:

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made PDE, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Guidance: ENISA sub requirements (not mandatory)

- Users should be made aware of the existence of security updates either via automatic distribution, popup, newsletter, etc;
- This notice should contain information about the fixed issues and instructions on how to apply;
- Security updates should be released free of charge.



Click inside this box to enable scrolling.

A41:
Timely Release and Free Distribution of Security Updates ensures that security patches and fixes are delivered promptly and without cost to all users. It prioritizes rapid remediation based on severity and maintains open availability so that every supported device or system can receive critical updates without restrictions.

T50:
Notification and Communication Tools provide secure and reliable channels for submitting and sharing vulnerability information and update notices. Mechanisms like RFC 9116 security.txt, encrypted email, and authenticated mailing systems ensure confidentiality and integrity, while standard communication channels support broad and accessible outreach when security updates or advisories are published.

T40:
Update Frameworks provide structured mechanisms for packaging, delivering, and verifying software or firmware updates with integrity and authenticity guarantees. Solutions like libostree use content-addressed storage, atomic upgrades, and cryptographic verification to ensure reliable, tamper-resistant update processes across devices and systems

Important PDEs

7.1

PDEs which have the **core functionality of a product category set out in Annex III** shall be considered to be **important PDEs and** shall be **subject to the conformity assessment procedures referred to in Article 32(2) and (3).**

Art. 32.2 and 3

Annex III - Class I

1. **Identity management systems** and **privileged access management software and hardware**, including authentication and access control readers, including biometric readers;
2. Standalone and embedded **browsers**;
3. **Password managers**;
4. **Software that searches for, removes, or quarantines malicious software**;
5. PDEs with the function of virtual private network **(VPN)**;
6. **Network management systems**;
7. Security information and event management **(SIEM) systems**;
8. **Boot managers**;
9. **Public key infrastructure and digital certificate issuance software**;
10. **Physical and virtual network interfaces**;
11. **Operating systems**;
12. **Routers, modems** intended for the connection to the internet, and switches;
13. **Microprocessors** with security-related functionalities;
14. **Microcontrollers** with security-related functionalities;
15. Application specific integrated circuits **(ASIC)** and field-programmable gate arrays **(FPGA)** with security-related functionalities;
16. **Smart home** general purpose virtual assistants;
17. **Smart home products with security functionalities**, including smart door locks, security cameras, baby monitoring systems and alarm systems;
18. **Internet connected toys** covered by Directive 2009/48/EC **that have social interactive features** (e.g. speaking or filming) **or that have location tracking features**;
19. **Personal wearable products to be worn or placed on a human body that have a health monitoring** (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, **or personal wearable products that are intended for the use by and for children**.

Annex III - Class II

1. **Hypervisors and container runtime systems** that support virtualised execution of operating systems and similar environments;
2. **Firewalls, intrusion detection and prevention systems**;
3. Tamper-resistant **microcontrollers**.
4. Tamper-resistant **microprocessors**;

If a PDE that has the core functionality of a product category set out in Annex III **is integrated into another product**, this does not automatically mean that the entire final product must go through the same conformity assessment procedures described in Article 32(2) and (3).

7.4: **Commission Implementing Regulation (EU) 2025/2392** specifies the technical description of the categories of PDEs under classes I and II as set out in Annex III.

Important PDEs

7.1

PDEs that have the core functionality of a product category set out in Annex III shall be considered to be important PDEs and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3).

7.2

Products that are **into classes I and II** as set out in Annex III, **must meet at least one** of the following **criteria**:

(a) **the PDE primarily performs functions that are critical to the cybersecurity of other products, networks or services**, for example, functions such as:

- securing authentication and access;
- intrusion prevention and detection;
- end-point security; or
- network protection.

(b) **the PDE performs a function that, if compromised, could pose a significant risk of adverse effects** because of its intensity and its ability to disrupt, control, **or cause damage to a large number of other products, or to the health, safety, or security of its users through direct manipulation.**

For example, such functions may include:

- central system functions,
- network management;
- configuration control;
- virtualisation; or
- the processing of personal data.

By defining objective criteria, the Regulation creates a risk-based classification system.

This approach ensures that cybersecurity obligations are proportionate: **products whose vulnerabilities, if exploited, could result in more severe consequences or broader systemic effects are subject to stricter conformity assessment procedures.**

Annex III - Class I → **Art. 32.2** Conformity assessment procedures

Annex III - Class II → **Art. 32.3** Conformity assessment procedures

7.3

The Commission has the power to update Annex III by means of delegated acts.

This means the Commission may:

- **add a new product category** within each class (I or II) **and define it** clearly;
- **move an existing product category from one class to another**; or
- **remove a product category from the list**.

When doing so, the Commission shall take into account:

- the **cybersecurity functions** of the products; **and**
- the **level of cybersecurity risk they pose**, according to the criteria above.

The delegated acts shall, where appropriate, provide for a minimum transitional period of 12 months, before the relevant conformity assessment procedures as referred to in Article 32(2) and (3) **start applying, unless a shorter transitional period is justified on imperative grounds of urgency.**

Critical PDEs

8

PDEs that have the core functionality of a product category set out in Annex IV shall be considered to be critical PDEs.
Where no delegated acts determining which critical PDE is required to obtain a European cybersecurity certificate have been adopted, they shall be subject to the conformity assessment procedure referred to in Article 32(3).

Art. 32.3

Annex **IV**

1. **Hardware Devices with Security Boxes**;
2. **Smart meter gateways** within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 **and other devices for advanced security purposes**, including for secure cryptoprocessing;
3. **Smartcards or similar devices, including secure elements**.

8.1

The Commission has the power **to adopt delegated acts** to determine which PDEs listed in Annex IV **must obtain a European cybersecurity certificate**.

Before adopting such delegated acts, the Commission must:

1. carry out an **assessment of the potential market impact** of the envisaged measures, **and**
2. carry out **consultations with relevant stakeholders.**

These delegated acts must:

1. **specify the required assurance level** that shall be proportionate to the level of cybersecurity risk associated with the PDEs; **and**
2. **take account of their intended purpose**, including the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555.

Where NO delegated acts have been adopted:
critical PDEs shall be subject to the conformity assessment procedures referred to in Article 32(3).

Where delegated acts have been adopted:
they shall provide for a **minimum transitional period** of **6 months**, **unless** a shorter transitional period is justified for imperative reasons of urgency.

The Commission has this power because critical products have a higher level of cybersecurity risk than default products.
For this reason, **they are required to obtain a certificate** that proves compliance.

This certification:

1) **must be at an assurance level of at least "substantial";**
2) **must be obtained under a European cybersecurity certification scheme** established by Regulation (EU) 2019/881 (Cybersecurity Act);

   This applies only if an EU cybersecurity certification scheme for those types of products **already exists under Regulation** (EU) 2019/881 **and is available for manufacturers to use**.

3) **demonstrates compliance with the essential cybersecurity requirements** described in Annex I, either fully or in part.

Critical PDEs

8 **PDEs that have the core functionality of a product category set out in Annex IV shall be considered to be critical PDEs. Where no delegated acts determining which critical PDE is required to obtain a European cybersecurity certificate have been adopted, they shall be subject to the conformity assessment procedure referred to in Article 32(3).**

Art. 32.3

Annex **IV**

1 **Hardware Devices with Security Boxes**;

2 **Smart meter gateways** within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 **and other devices for advanced security purposes**, including for secure cryptoprocessing;

3 **Smartcards or similar devices, including secure elements**.

8.2

The Commission has the power to adopt **delegated acts to amend Annex IV by adding or withdrawing categories** of critical PDEs.

⇨ **Before adopting such delegated acts, the Commission must:**

1 carry out an **assessment of the potential market impact** of the envisaged measures, **and**

2 carry out **consultations** with relevant **stakeholders.**

⇨ **When determining such categories of critical PDEs and the required assurance level, the Commission must:**

1 take into account the 2 **criteria** referred to **in Article 7(2)**; **and**

2 **ensure that the categories of PDEs meet at least one of the following criteria:**

(a) **essential entities** (as defined in the Art. 3, NIS 2 Directive) **critically depend on that PDEs category; or**

(b) **incidents and exploited vulnerabilities** concerning that category could lead to **serious disruptions of critical supply chains** across the internal market.

Art. 7.2

Where delegated acts have been adopted:

they shall provide for a **minimum transitional period** of **6 months**, **unless** a shorter transitional period is justified for imperative reasons of urgency.

7.4

On 28 November 2025, the Commission adopted the Implementing Regulation (EU) 2025/2392 specifying the technical description of the categories of important and critical PDEs.

11

Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation (EU) 2023/988 shall **apply to PDEs with respect to aspects and risks or categories of risks that are not covered by this Regulation**

⇨ **where those products are not subject to specific safety requirements laid down in other 'Union harmonisation legislation'.**

When is a high-risk AI system - that is also a PDEs under the CRA - considered to be compliant with AIA cybersecurity rules?

12

If a PDEs is classified **as high-risk AI system,** it is considered to be **compliant with the AI Act's Art. 15 cybersecurity requirements** if:

(a) It meets the essential cybersecurity requirements in Annex I, Part I of the CRA;

(b) The manufacturer's internal processes comply with the essential cybersecurity requirements set out in Part II of Annex I of the CRA;

(c) This cybersecurity level required by Art. 15 AIA is declared in the EU declaration of conformity issued under the CRA.

12.2	High-risk AI systems **which are PDEs**	**Comply with Art. 15 AIA Cybesecurity requirements**	1) comply with CRA Annex I ERs; 2) CRA EU declaration conformity.	**Art. 43 AIA conformity assessment procedure** by AIA notified bodies
12.3	High-risk AI systems (to which **internal control assessment procedure applies**) which are **important** or **critical PDEs**	**Comply with Art. 15 AIA Cybesecurity requirements**	1) comply with CRA Annex I ERs; 2) CRA EU declaration conformity.	**Important/critical CRA conformity assessment** re. Annex I CRA ERs

This article explains the interplay between the CRA and the AI Act with particular regard to the conformity assessment procedure **PDEs classified as high-risk AI systems** must follow.

Article 13 consists of twenty-five paragraphs. To make its content clearer, this section groups the related obligations according to the **three main phases of the product lifecycle**, therefore **showing exactly when each obligation must be fulfilled by manufacturers** and how these requirements interconnect throughout the process.
Under the light-blue bar "**During all these stages**," you will find the obligations that **manufacturers must comply with at all times**, regardless of the phase of the product lifecycle.

➪ To fully understand Article 13, always refer to the specific lifecycle phase in which each obligation is placed.

Planning, design, development, production

- (13.1,2,3) **The cybersecurity risk assessment**;
- (13.5 and 6) **Vulnerabilities** - Table 1;
- (13.8) **How to determine the support period** - Table 1;
- (13.8) **How to determine the support period** - Table 2;
- (13.12) **Product compliance management**.

Delivery to the market

- (13.4) **The cybersecurity risk assessment**;
- (13.8) **Vulnerabilities** - Table 2;
- (13.21 and 24) **Corrective measures**;
- (13.15-16-19) **Manufacturers' information obligations towards users** - Table 1;
- (13.17-18-20-23) **Manufacturers' information obligations towards users** - Table 2.

Maintenance

- (13.3,7) **The cybersecurity risk assessment**;
- (13.8) **Vulnerabilities** - Table 2;
- (13.9) **Security update**;
- (13.10 and 11) **Versions**;
- (13.21 and 24) **Corrective measures**;
- (13.15-16-19) **Manufacturers' information obligations towards users** - Table 1;
- (13.17-18-20-23) **Manufacturers' information obligations towards users** - Table 2.

During all these stages

- (13.2) **The cybersecurity risk assessment**;
- (13.2 and 8) **Vulnerabilities** - Table 2;
- (13.14) **Product compliance management**;
- (13.13-22-23-25) **Manufacturers' information obligations towards authorities**.

The cybersecurity risk assessment - Table 1

Planning, design, development, production | Delivery to the market | Maintenance

13.1

Manufacturers **must design, process, develop and produce the PDEs in accordance with the essential cybersecurity requirements** set out in Part I of Annex I.

Annex I, part 1

13.2

To do this, manufacturers **must assess the cybersecurity risks of their PDEs.**

13.3

The cybersecurity risk assessment shall be documented and updated.

This assessment shall **comprise at least an analysis** of cybersecurity risks **based on**:

1) the **intended purpose** of the PDEs;
2) the **reasonably foreseeable** use of the PDEs;
3) the **conditions of use** of the PDEs, such as the operational environment **or** the assets to be protected;

taking into account **the length of time the product is expected to be in use**.

And it shall **indicate**:

1) **Whether** and, **if so in what manner**:
   - the **security requirements** set out in Part I, point (2), of Annex I **are applicable to the relevant PDEs**; **and**
   - **how those requirements are implemented** as informed by the cybersecurity risk assessment.

2) **How** the manufacturer **is to apply**:
   - Annex I, part I, point 1: "PDEs shall be designed, developed and produced in such a way that they **ensure an appropriate level of cybersecurity based on the risks**".
   - Annex I, part II: the **vulnerability handling requirements**.

Annex I, part 1

Annex I, part 2

The cybersecurity risk assessment - Table 2

Delivery to the market

13.4

Once ready, the manufacturer shall **include the cybersecurity risk assessment in the technical documentation** required pursuant to Article 31 and Annex VII.

Art. 31
Technical documentation

Where **certain essential cybersecurity requirements are not applicable** to the PDEs, the manufacturer shall **include a clear justification** to that effect in that technical documentation.

For PDEs as referred to in Article 12 - **High-risk AI systems** - which are also subject to other Union legal acts, **the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts.**

Art. 12
High-risk AI systems

Maintenance

13.3

The **cybersecurity risk assessment** - carried out during the red phase - **shall be documented and updated** as appropriate **during a support period**.

13.7

Whether:

1
relevant cybersecurity aspects
concerning the PDEs **are discovered**; or

2
vulnerabilities of which they **become aware**; or

3
and **any relevant information provided** by third parties

The **cybersecurity risk assessment**
- carried out during the red phase -
shall be documented and updated.

Example

During all these stages

13.2

Manufacturers **take the outcome of that assessment** of the cybersecurity risks associated with a PDEs - made during the red phase - **into account during the planning, design, development, production, delivery and maintenance phases** of the PDEs (13.2).

With a view to:

- **minimising cybersecurity risks**;
- **preventing incidents and minimising their impact,** including in relation to the health and safety of users.

Planning, design, development, production | Delivery to the market | Maintenance

13.5

Manufacturers shall **exercise due diligence** **when integrating components sourced from third parties** so that those components **do not** compromise the cybersecurity of the PDEs

including when integrating components of FOSS that have **not** been made available on the market in the course of a commercial activity.

13.6

Upon **identifying** **a vulnerability** in a component, **including in an open source-component**, which is integrated in the PDEs, manufacturers shall:

1) report **the vulnerability** to the person or entity manufacturing or maintaining the component, and

2) address and remediate **the vulnerability** in accordance with the vulnerability handling requirements set out in Part II of Annex I.

Annex I, part 2

Where manufacturers have developed **a software or hardware modification to address the vulnerability** in that component

They shall **share the relevant code or documentation** with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.

ECFAQ:
If the manufacturer of a PDEs is aware that an integrated component contains a vulnerability, but that vulnerability cannot be exploited in its PDEs, that vulnerability is not actively exploited, and therefore it is not subject to mandatory reporting.
Manufacturers can still notify that vulnerability on a voluntary basis, in accordance with Article 15, and are required to report the vulnerability to the person or entity manufacturing or maintaining the component, in accordance with Article 13(6).

Vulnerabilities - Table 2

Delivery to the market | **Maintenance**

13.8

Manufacturers shall **ensure**, when placing a PDEs on the market, and for the support period, **that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements** set out in Part II of Annex I.

Annex I, part 2

During all these stages

13.2

Manufacturers shall **systematically document**, in a manner that is **proportionate to the nature and the cybersecurity risks**:

- **relevant cybersecurity aspects** concerning the PDEs;
- **vulnerabilities** of which they become **aware**;
- and **any relevant information** provided **by third parties**.

and shall, **where applicable, update the cybersecurity risk assessment** of the products.

13.8(6)

Manufacturers shall have **appropriate policies and procedures**, including **coordinated vulnerability disclosure policies**, referred to in Part II, point (5), of Annex I → **to process and remediate potential vulnerabilities** in the PDEs reported from internal or external sources.

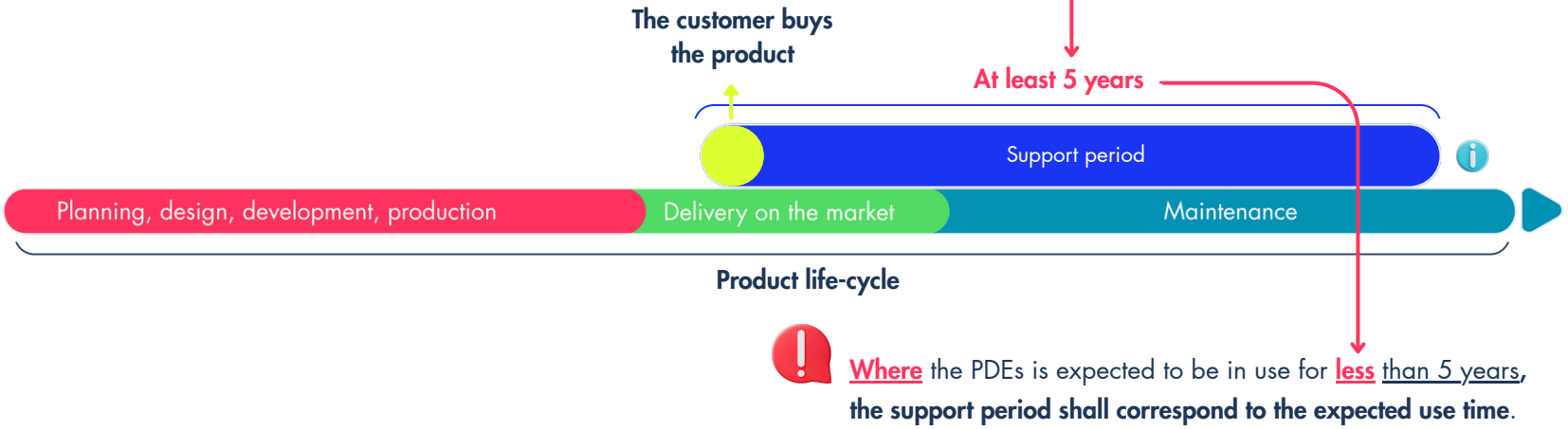
Annex I, **part 2, point 5**

"Manufacturers of PDEs shall **put in place and enforce a policy on coordinated vulnerability disclosure**;"

Planning, design, development, production | Delivery to the market | Maintenance

13.8(3)

The support period shall be **at least 5 years**



Where the PDEs is expected to be in use for **less** than 5 years, **the support period shall correspond to the expected use time**.

Example

How to determine the support period - Table 2

Planning, design, development, production | Delivery to the market | Maintenance

13.8(2)

Manufacturers shall **determine the support period** so that it **reflects the length of time during which the product is expected to be in use**, taking into account:

1) **reasonable user expectations**;

2) the **nature** of the product;

3) including its **intended purpose**; as well as

4) **relevant Union law** determining the lifetime of PDEs.

Manufacturers **may also** take into account:

5) the support periods of PDEs offering a similar functionality placed on the market by other manufacturers;

6) the availability of the operating environment;

7) the support periods of integrated components that provide core functions and are sourced from third parties; as well as

8) relevant guidance provided by the Dedicated Administrative Cooperation Group (ADCO) established pursuant to Article 52(15) and the Commission.

The matters to be taken into account in order to determine the support period **shall be considered in a manner that ensures proportionality**.

13.8(5)

Manufacturers shall include the information that was taken into account to determine the support period of a PDEs in the **technical documentation** as set out in Annex VII.

13.8(5)

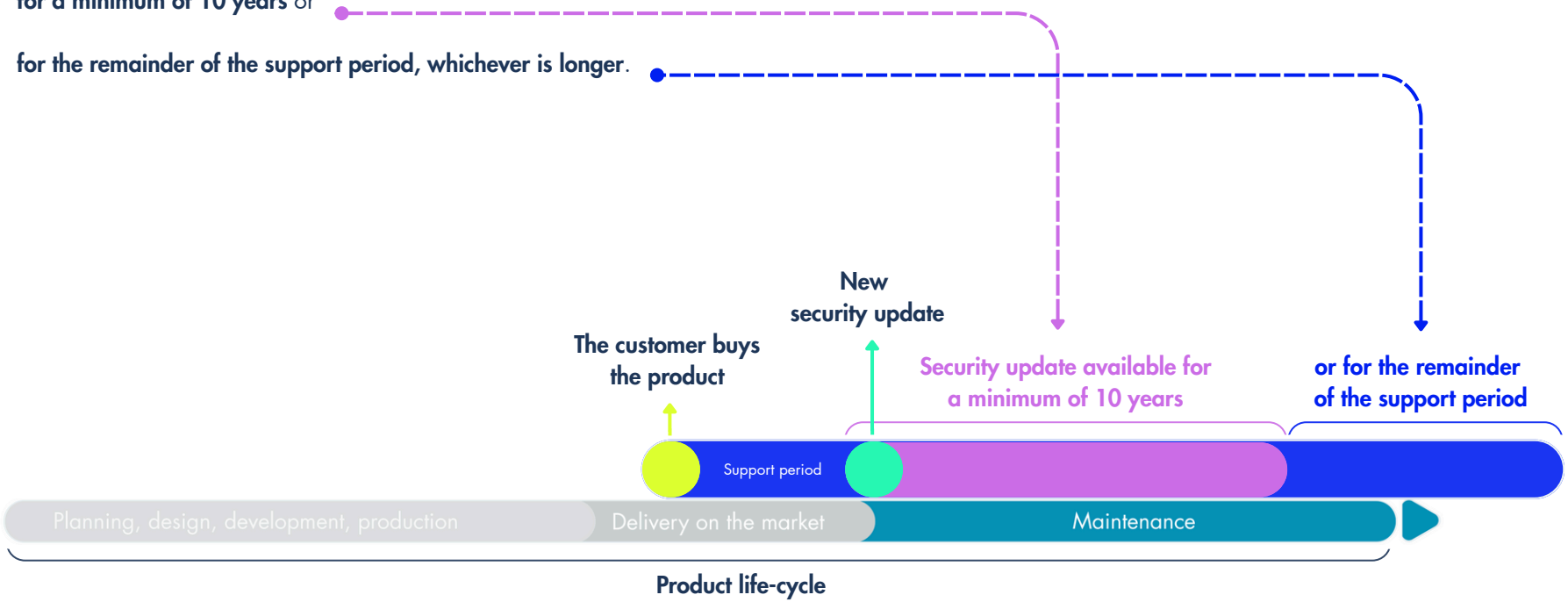
The **Commission may adopt delegated acts by specifying the minimum support period** for specific product categories **where** the market surveillance data suggests inadequate support periods.

Delivery to the market | Maintenance

13.9

Manufacturers shall **ensure that each security update**, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, **remains available** after it has been issued:

- **for a minimum of 10 years** or
- **for the remainder of the support period, whichever is longer**.



Annex I, **part 2, point 8**

"Manufacturers of PDEs shall ensure that **security updates available to address identified security issues 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 - unless otherwise agreed** between a manufacturer and a business user in relation to a tailor-made PDEs".

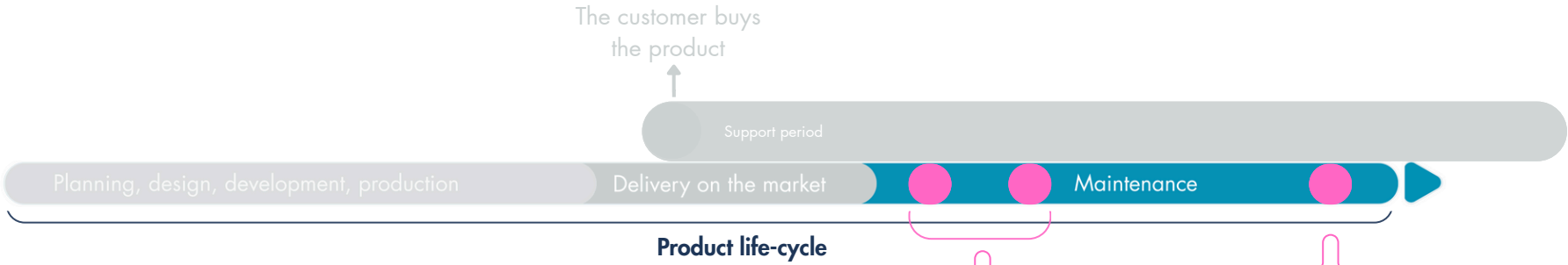
Delivery to the market | Maintenance

13.10

Where a manufacturer has placed **subsequent substantially modified versions** (pink points in the table) of a software product on the market that manufacturer **may ensure compliance with the essential cybersecurity requirement** set out in Part II, point (2), of Annex I **only for the version that it has last placed** on the market

Annex I, **part 2, point 2**

"Manufacturers of PDEs shall address and remediate vulnerabilities:
- **without delay**,
- **providing security updates,** separately from functionality updates - **where technically feasible**"



provided that the **users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs** to adjust the hardware and software environment in which they use the original version of that product.

subsequent substantially modified versions of a software previously placed on the market

these may not be compliant with that requirement

It is possible to comply with the requirement only with regard to the latest substantially modified version

Free access to users of the versions that were previously placed on the market

13.11

Manufacturers **may maintain public software archives enhancing user access to historical versions**.

In those cases, **users shall be clearly informed** in an easily accessible manner **about risks associated with using unsupported software**.

Planning, design, development, production | Delivery to the market | Maintenance

13.12

Before placing a PDEs on the market, manufacturers shall **draw up the technical documentation** referred to in Article 31.

Art. 31

13.12

Manufacturers shall **carry out the chosen conformity assessment procedures** as referred to in Article 32 or have them carried out.

Where the conformity assessment procedure demonstrates compliance of the PDEs with:

1) the essential cybersecurity **requirements** set out in Part I of Annex I; and

2) of the **processes** put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I.

Manufacturers shall draw up the EU declaration of conformity in accordance with Article 28;

and **affix the CE marking** in accordance with Article 30.

Art. 32 | Annex I, Part I | Annex I, Part II | Art. 28 | Art. 30

During all these stages

13.14

Manufacturers shall ensure that procedures are in place for PDEs that are part of a series of production to remain in conformity with this Regulation.

Manufacturers shall **adequately take into account**:

- **changes** in the development and production process or in the design or characteristics of the **PDEs**; and
- **changes** in the **harmonised standards**, European cybersecurity certification **schemes** or **common specifications** as referred to in Article 27 by reference to which the conformity of the PDEs is declared or by application of which its conformity is verified.

Art. 27

Delivery to the market | Maintenance

13.21

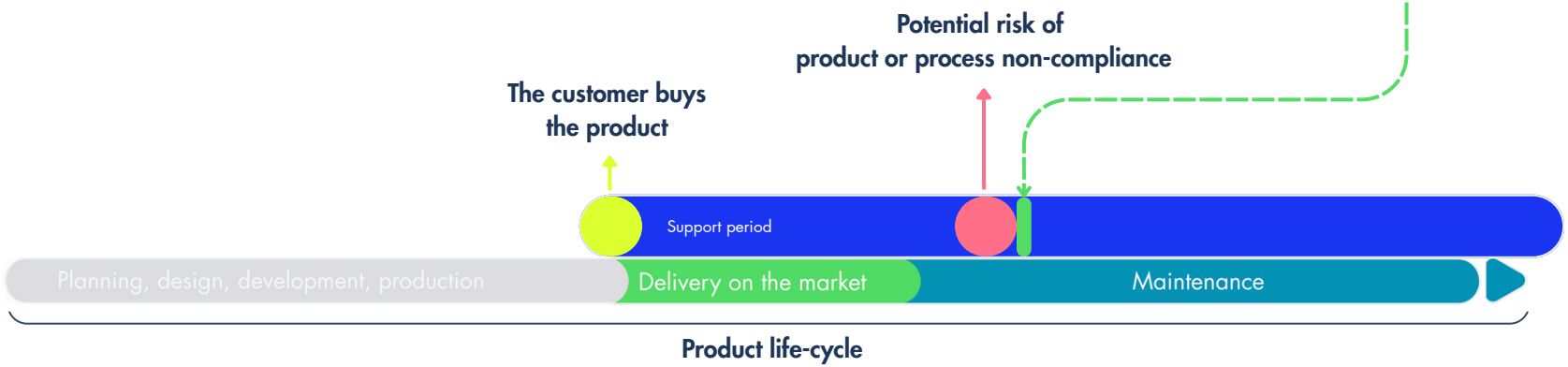
From the placing on the market and for the support period, manufacturers **who know or have reason to believe that**:

- the PDEs or
- the processes

are not in conformity with the essential cybersecurity requirements set out in Annex I

shall **immediately**:

1) **take the corrective measures** necessary to bring that PDEs or the manufacturer's processes into conformity; or as appropriate:
2) **to withdraw the product**; or
3) **recall the product**.



Annex I, Part I

Manufacturers' information obligations towards authorities

During all these stages

Retention of documentation

13.13

Manufacturers shall **keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities:**

- **for at least 10 years after the PDEs has been placed on the market;**
- **or for the support period,** whichever is longer.

Provision of information and cooperation

13.22

Upon a reasoned request from a market surveillance authority, manufacturers shall **provide that authority with all the necessary information and documentation,** in paper or electronic form, **to demonstrate the conformity**:

- **of the PDEs,** and
- **of the processes put in place**.

Also, at the authorities request, manufacturers shall cooperate with them, on any measures taken to eliminate the cybersecurity risks posed by the PDEs which they have placed on the market.

13.25

Market surveillance authorities may request manufacturers of specific categories of PDEs to provide the relevant SBOMs, to understand what software (including open-source) their products depend on. The information is collected and analyzed at EU level **in an anonymous and aggregated way**.

Manufacturer's cessation of operations

13.23

A manufacturer that ceases its operations, and, because it is not able to comply with this Regulation, **shall inform the users** of the relevant PDEs **of the impending cessation of operations**.

- **before** the cessation of operations takes effect;
- **by any means available, and**
- **to the extent possible**.

13.24

The Commission may specify the format and elements of the Software Bill Of Materials - SBOM referred to in Part II, point (1), of Annex I.

Annex I, Part 2, point 1

Manufacturers' information obligations towards users - Table 1

Delivery to the market | Maintenance

Product identification

13.15

The **PDEs must bear elements allowing their identification**:

1. a type;
2. batch, **or** serial number, **or** other identification elements;

or where that is not possible, that **information is provided on their packaging or in a document** accompanying the PDEs.

Support period

13.19

The end date of the support period - **at least** the month and the year - **must be clearly and understandably specified at the time of purchase in an easily accessible manner.**

Where applicable, this date must be clearly and understandably **specified**:

- **on the PDEs,**
- **its packaging, or by digital means.**

Where technically feasible in light of the nature of the PDEs

- manufacturers shall **display a notification to users** informing them that their PDEs has **reached the end of its support period**.

Art. 13.8

Manufacturer identification

13.16

Manufacturers shall **indicate contact details**:

1. the name;
2. registered trade name **or** registered trademark of the manufacturer; **and**
3. the postal address;
4. email address **or** other digital contact details;
5. **where applicable**, the website where the manufacturer can be contacted

- **on the PDEs**;
- **on its packaging or in a document** accompanying the PDEs;
- **Also, in the information and instructions to the user** set out in Annex II.

In a language which can be **easily understood**.

Manufacturers' information obligations towards users - Table 2

Delivery to the market | Maintenance

User instructions

13.18

The PDEs are accompanied by the information and instructions to the user set out in Annex II.

They shall be **in paper or electronic form**, in an easily understandable language. They shall be **clear** and **legible**.

They shall allow for:
- **the secure installation**,
- **operation** and
- **use** of PDEs.

Manufacturers shall **keep** the information and instructions **at the disposal**:
- for **at least 10 years after** the PDEs has been placed on the market; **or**
- **for the support period**, whichever is longer.

Where the information and instructions are provided **online**, manufacturers shall ensure that they are **accessible**, **user-friendly** and **available online** for the **same period**.

User contact and support

13.17

Manufacturers shall **designate a single point of contact. It must be:**

1) **easily identifiable by the users; and**
2) **included in the information and instructions to the user** set out in Annex II.

to enable users to **communicate directly and rapidly with them;** and

to facilitate **reporting on vulnerabilities** of the PDEs.

to **allow users to choose their preferred means of communication** and shall **not limit such means to automated tools**.

EU declaration of conformity

13.20

Manufacturers shall **provide the PDEs with a copy:**
- of the **EU declaration of conformity**, **or**
- a **simplified EU declaration of conformity.**

If manufacturers provide a simplified declaration, **it must show the exact web address of the full declaration**.

Manufacturer's cessation of operations

13.23

A manufacturer that ceases its operations, and, because **it is not able to comply** with this Regulation, shall **inform the users** of the relevant PDEs **of the impending cessation of operations**.

before the cessation of operations takes effect;

- **by any means available, and**
- **to the extent possible**.

Article 14 ⇨ **Mandatory** reporting

- (Art. 14.1-2-6) **Reporting exploited vulnerabilities;**
- (Art. 14.3-4-5-6) **Reporting severe security incident;**
- (Art. 14.7) **The coordinating CSIRT;**
- (Art. 14.8) **Informing users.**

Article 15 ⇨ **Voluntary** reporting

- (Art. 15.1,2,3) **Voluntary reporting of cybersecurity issues** - Table 1;
- (Art. 15.4,5) **Voluntary reporting of cybersecurity issues** - Table 2;
- (Art.14.1,3 - 15.1,2 - 16.1 - 14.7) **How mandatory and voluntary notifications are handled** - Table 1.

Article 16 ⇨ **Single reporting platform** and **exceptional circumstances**

- (Art.16.2 - 16.3) **How mandatory and voluntary notifications are handled** - Table 2;
- (Art. 16.2) **Exceptional circumstances: dissemination delayed or limited** - Table 1;
- (Art. 16.2) **Exceptional circumstances: dissemination delayed or limited** - Table 2;
- (Art. 16.6) **Exceptional circumstances: dissemination delayed or limited** - Table 3.

14.9

By **11 December 2025**: the Commission adopts delegated acts specifying **when the dissemination of notifications can be delayed on cybersecurity grounds**.

14.10

The Commission may, by means of implementing acts, **specify further the format and procedures of the notifications.**

Reporting exploited vulnerabilities

14.1

If a manufacturer becomes aware of an actively exploited vulnerability contained in the PDEs, it must notify it simultaneously to:

- **the CSIRT designated as coordinator** of the Member State where the manufacturer has **its main establishment** in the Union, **and**
- **ENISA.**

⇨ **using the single reporting platform.**

Art. 16
Single Reporting Platform

14.2

So, from the moment a manufacturer becomes aware of an actively exploited vulnerability, it must:

A) in any event within 24 hours ⇨ send an **early warning notification** indicating, **where applicable**, the **Member States** in which the manufacturer is aware that its **PDEs is available** on the market;

B) in any event within 72 hours ⇨ submit a **vulnerability notification**, which shall provide:

1. general information, **as available**, about the PDEs;
2. the general **nature of the exploit** and of the **vulnerability**;
3. **any corrective or mitigating measures taken**; and
4. **corrective or mitigating measures that users can take**; and
5. where applicable, an **indication of the sensitivity of that information**.

C) no later than 14 days after a corrective or mitigating measure is available ⇨ submit a **final report** including **at least** the following:

- a **description of the vulnerability**, including its severity and impact;
- where available, **information concerning any malicious actor** that has exploited or that is exploiting the vulnerability;
- **details about the security update or other corrective measures** that have been made available to remedy the vulnerability.

The manufacturer must provide the required information as soon as it becomes available.

The deadlines of 24 hours, 72 hours and 14 days represent the latest possible time limits.

14.6

D) If necessary and if requested by the CSIRT designated as coordinator ⇨ provide an **intermediate report on relevant status updates** about the actively exploited vulnerability of the PDEs.

Reporting severe security incident

14.3

If a manufacturer **becomes aware** of **any severe incident having an impact on the security** of the PDEs, it must notify it **simultaneously** to:

- **the CSIRT designated as coordinator** of the Member State where the manufacturer has its main establishment in the Union, **and**
- **ENISA.**

⇨ **using the single reporting platform.**

Art. 14.5
Definition of severe incident

Art. 16
Single Reporting Platform

14.4

So, from the moment a manufacturer becomes aware of any severe incident having an impact on the security of the PDEs, it must:

A) in any event within 24 hours ⇨ send an **early warning notification** indicating:

- **at least**, whether the incident is **suspected of being caused by unlawful or malicious acts;**
- **where applicable**, **the Member States** in which the manufacturer is aware that its **PDEs is available** on the market.

B) in any event within 72 hours ⇨ submit a **incident notification**, which shall provide:

1. general information, where available, about the **nature of the incident**;
2. an initial **assessment** of the incident; as well as any
3. **corrective or mitigating measures taken**, and
4. **corrective or mitigating measures that users can take**,
5. where applicable, an indication of the sensitivity of that information.

C) If the incident notification has been submitted, then within 1 month ⇨ submit a **final report** including **at least** the following:

- a **detailed description of the incident**, including its severity and impact;
- the type of threat or root cause that is likely to have triggered the incident;
- applied and ongoing mitigation measures.

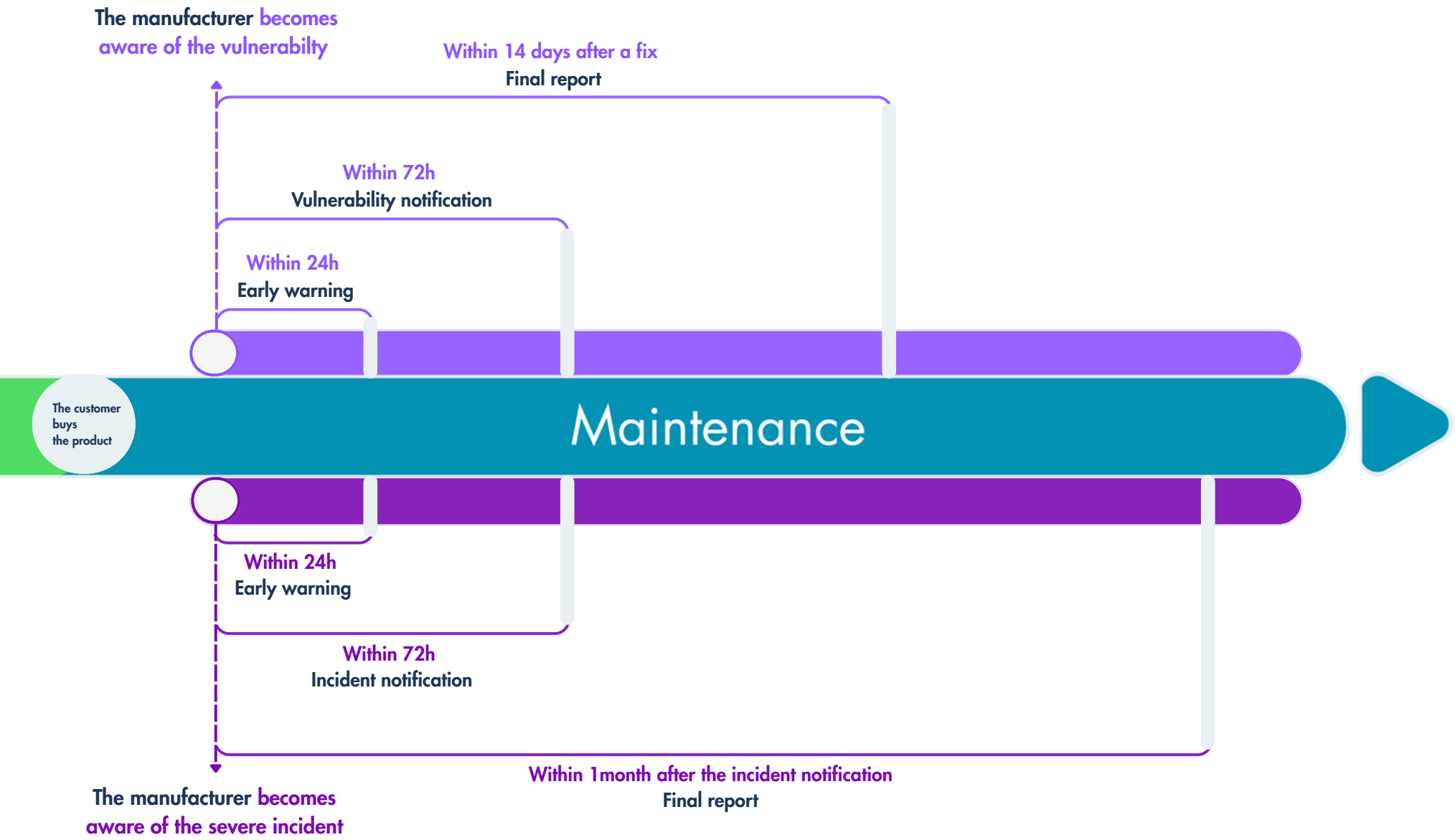
The manufacturer must provide the required information as soon as it becomes available.

The deadlines of 24 hours, 72 hours and 1 month represent the latest possible time limits.

14.6

D) If necessary and if requested by the CSIRT designated as coordinator ⇨ provide an **intermediate report on relevant status updates** about the severe incident having an impact on the security of the PDEs.

Overview: mandatory reporting



14.9

By **11 December 2025**: the Commission adopts delegated acts specifying **when the dissemination of notifications can be delayed on cybersecurity grounds**.

14.10

The Commission may, by means of implementing acts, **specify further the format and procedures of the notifications.**

14.7

All notifications (about vulnerabilities or severe incidents) **must** be submitted via **the single reporting platform**, using one of the electronic notification end-points of that platform.

The notification must be submitted **to**:

- the **CSIRT designated as coordinator** of the Member State where the manufacturer has its **main establishment** in the Union.
- **at the same time, the notification is made accessible to ENISA.**

Art. 16
Single Reporting Platform

How to determine the coordinating CSIRT

A manufacturer has its main establishment in the Member State **where decisions on the cybersecurity of the PDEs are are predominantly taken**.

If such a Member State cannot be determined

- the main establishment shall be considered to be in the Member State where the manufacturer has the establishment with the **highest number of employees** in the Union.

If a manufacturer has no main establishment in the Union

- then it must submit the notification to the coordinating CSIRT of the **Member State determined** in this order of priority:

a) The Member State of the **authorised representative** with the highest number of its PDEs.

b) The Member State of the **importer** placing on the market the highest number of its PDEs.

c) The Member State of the **distributor** making available on the market the highest number of its PDEs;

d) The Member State in which the **highest number of users** of its PDEs are located. A manufacturer **may submit** notifications related to **any** subsequent actively exploited vulnerability **or** severe incident to the same CSIRT designated as coordinator to which it first reported.

Art. 18
Authorised Representative

- **Once the manufacturer has chosen a CSIRT under point (d), it may use the same CSIRT for future notifications.**

14.8

If a manufacturer **becomes aware** of an **actively exploited vulnerability** or **a severe incident** having an **impact** on the security of the PDEs, **it must inform** about the vulnerability or incident

- **the impacted users, and**
- **where appropriate all users.**

Where necessary, the manufacturer also provides instructions on any **risk mitigation and corrective measures** that the users can deploy to mitigate the impact of that vulnerability or incident, in a structured, machine-readable format.

Where the manufacturer fails to inform the users of PDEs in a timely manner,
the notified CSIRTs designated as coordinators **may provide such information to the users.**

Voluntary reporting of cybersecurity issues - Table 1

15.1, 2 and 3

Manufacturers

Legal persons other than the manufacturer

Natural persons other than the manufacturer

may notify on a voluntary basis

1. **any vulnerability contained in a PDEs;**
2. **cyber threats that could affect the risk profile of a PDEs;**
3. **any incident having an impact on the security of the PDEs;**
4. **near misses that could have resulted in such an incident.**

through the single reporting platform

The CSIRT designated as coordinator

It may prioritise the processing of mandatory notifications over voluntary notifications.

OR

ENISA

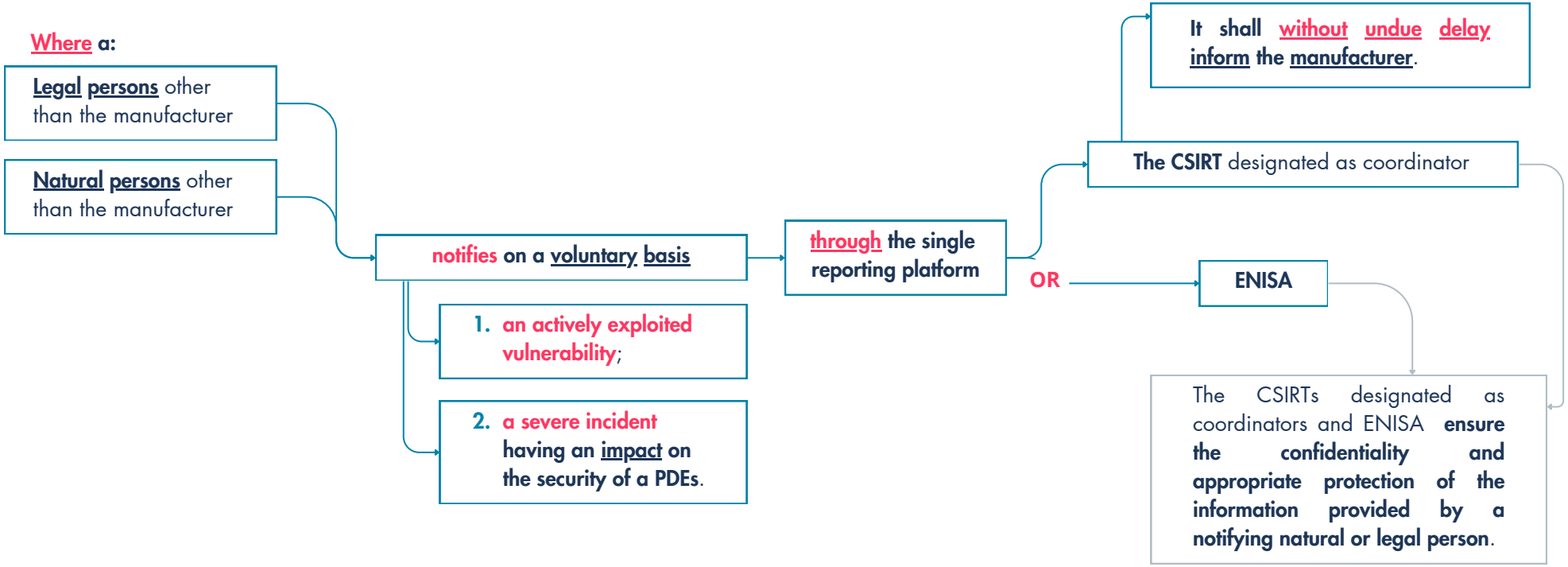
The CSIRT designated as coordinator or ENISA shall **process the notifications in accordance with the procedure laid down in Article 16.**

Art. 16

14.10

The Commission may, by means of implementing acts, **specify further the format and procedures of the notifications.**

15.4 and 5



If natural or legal persons report voluntarily, they will not have any additional obligations because of that report. They will only be subject to the same obligations they would have had even without submitting it, without prejudice to the prevention, investigation, detection and prosecution of criminal offences.

How mandatory and voluntary notifications are handled - Table 1

Mandatory reporting apply only to the manufacturer

14.1 and 3

If a manufacturer becomes aware of:

- an actively exploited vulnerability contained in the PDEs;
- any severe incident having an impact on the security of the PDEs.

Voluntary reporting – all actors

15.1and 2

Manufacturers as well as other natural or legal persons may notify on a voluntary basis:

- any vulnerability contained in a PDEs;
- cyber threats that could affect the risk profile of a PDEs;
- any incident having an impact on the security of the PDEs;
- near misses that could have resulted in such an incident.

16.1

They **must submit both** mandatory and voluntary notifications **via the** EU single reporting platform.

16.1,4,5

The platform is established and managed by ENISA.

TO

The CSIRT designated as coordinator

AND

where mandatory reporting, simultaneously to ENISA

OR

where voluntary reporting, to ENISA

14.7

The CSIRT designated as coordinator **is the CSIRT of the Member State where the manufacturers have their main establishment in the Union**, that is in the Member State **where the decisions related to the cybersecurity of its PDEs are predominantly taken**.

How mandatory and voluntary notifications are handled - Table 2

16.2

After receiving a notification, the CSIRT designated as coordinator initially receiving the notification, without delay, disseminates the notification

via the single reporting platform — TO → the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the PDEs has been made available.

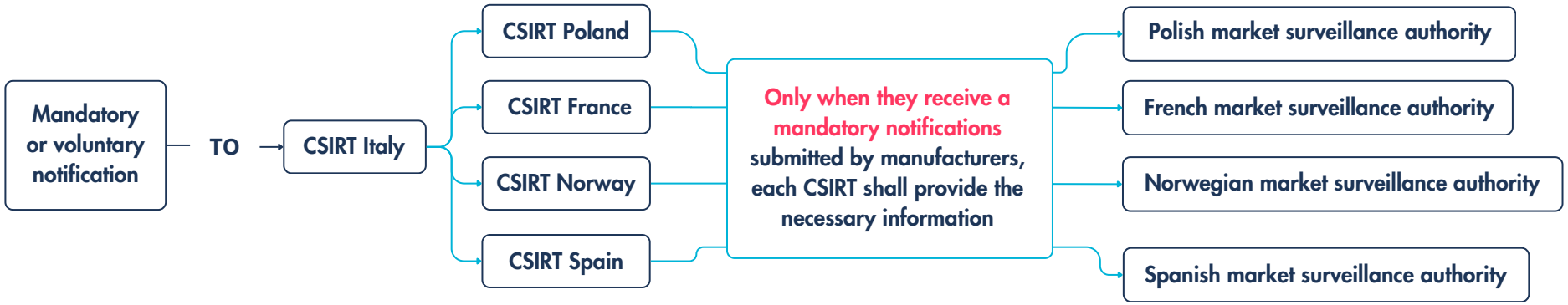
16.3

Only when they receive a notification of:

- an actively exploited vulnerability in a PDEs, or
- a severe incident having an impact on the security of a PDEs

⇨ Those coordinating CSIRTs provide the necessary information to their national market surveillance authorities to help them fulfil their responsibilities under this Regulation.

Example



This steps ensure that all relevant national authorities are informed quickly and consistently.

Exceptional circumstances: dissemination delayed or limited - Table 1

16.2

Standard rule: the CSIRT that first receives a notification must disseminate it immediately to the other CSIRTs through the EU reporting platform.

BUT → **A manufacturer may request the CSIRT designated as coordinator** - that is the one that first receives the notification - **to delay the dissemination of that notification.**

The manufacturer can **make such a request when**:

- **The vulnerability is already being managed** under a coordinated vulnerability disclosure process; or
- **The information is highly sensitive**, and immediate sharing could create or worsen cybersecurity risks.

This request can be made **only for**:

- **specific cybersecurity-related reasons, and**
- **as long as strictly necessary** to avoid further risks.

After receiving the request, the CSIRT designated as coordinator **may decide to withholding a notification** but **only if** it finds the **reasons justified**. **In that case, the CSIRT must:**

- **immediately inform ENISA of its decision;**
- **provide a justification for withholding the notification; and**
- **indicate when the notification will be shared** according to the normal dissemination procedure.

Exceptional circumstances: dissemination delayed or limited - Table 2

16.2

Standard rule: the CSIRT that first receives a notification must disseminate it immediately to the other CSIRTs through the EU reporting platform.

BUT

The manufacturer may indicate in its notification that:

1) the vulnerability has been **actively exploited by a malicious actor** and, based on available information, **the exploit has occurred only in the Member State of the CSIRT that received the notification**;

2) **immediate dissemination** of the notification **would likely reveal information** that could harm the essential interests of that Member State; **or**

3) **dissemination would itself create an imminent and serious cybersecurity risk.**

In such cases, **the CSIRT** designated as coordinator **does not share the full notification immediately**.

Once the exceptional circumstances no longer apply, the CSIRT designated as coordinator **must send the complete notification to ENISA and to the other CSIRTs concerned.**

Instead, it provides to ENISA only limited information, namely:

A) that a **notification** has been **submitted by the manufacturer**;

B) **general details** about the affected **product**;

C) a **summary of the exploit's nature**, **and**

D) a **note** stating that security-related grounds have been invoked to delay full dissemination.

If, based on the limited information received, **ENISA believes there is a systemic risk for cybersecurity in the EU internal market, it may recommend that the CSIRT** designated as coordinator **disseminate the full notification to all CSIRTs and to ENISA itself.**

Exceptional circumstances: dissemination delayed or limited - Table 3

16.6

Standard rule: the CSIRT that first receives a notification must disseminate it immediately to the other CSIRTs through the EU reporting platform.

BUT → If a CSIRT designated as coordinator becomes aware of an actively exploited vulnerability as part of a coordinated vulnerability disclosure (CVD) process, as referred to in Article 12(1) of Directive (EU) 2022/2555, that CSIRT (the one that first received the notification) may delay the dissemination of the relevant notification via the single reporting platform.

Such a delay is allowed only for:

- cybersecurity-related reasons and only for
- as long as strictly necessary;
- until the parties involved in the coordinated vulnerability disclosure give their consent to share the information.

BUT → This rule does not prevent manufacturers from voluntarily notifying the same vulnerability following the procedure set out in this Article.

Reporting: what else is important to keep in mind?

No increased liability for reporting

17.4

The mere act of notification in accordance with Arts. 14(1) and (3) or Article 15(1) and (2) **shall not subject the notifying natural or legal person to increased liability.**

Public information in case of severe incidents

17.2

Where public awareness is necessary

- to prevent or mitigate a severe incident having an impact on the security of the PDEs, **or**
- to handle an ongoing incident, **or**
- where disclosure of the incident is otherwise in the public interest,

the CSIRT designated as coordinator of the relevant Member State may, after consulting the manufacturer concerned and, **where appropriate**, in cooperation with ENISA, **inform the public about the incident or require the manufacturer to do so.**

Updating the European vulnerability database

17.5

After a security update or another form of corrective or mitigating measure is available, **ENISA shall, in agreement with the manufacturer** of the PDEs concerned, **add the publicly known vulnerability** notified pursuant to Article 14(1) or Article 15(1) **to the European vulnerability database.**

Support for manufacturers, especially SMEs

17.6

The CSIRTs designated as coordinators shall provide helpdesk support in relation to the reporting obligations pursuant to Article 14 **to manufacturers** and in particular manufacturers that qualify as microenterprises or as small or medium-sized enterprises.

ENISA's recurring reporting obligation and sharing information with EU-level coordination bodies

17.1 and 3

ENISA may share relevant information received through mandatory or voluntary notifications (Arts. 14 and 15) **with EU-CyCLONe, only when the information is considered useful for the coordinated management of large-scale cybersecurity incidents or crises.**

Every 24 months, ENISA shall prepare a technical report on emerging trends regarding to cybersecurity risks in PDEs.
This report is based on notifications received under Arts. 14(1),(3) and 15(1),(2) **and is submitted to the NIS Cooperation Group.**
The first report shall be submitted within 24 months from the date when the reporting obligations under Article 14(1),(3) start to apply.

18

A manufacturer may, by a written mandate, appoint an authorised representative.

BUT → **The obligations laid down in** Article **13(1) to (11),** Article **13(12), first subparagraph, and** Article **13(14) shall not form part of the authorised representative's mandate.**

→ **Therefore, the authorised representative is not required to:**

13.1	ensure secure design, development, production;
13.2	perform or oversee the product's cybersecurity risk assessment;
13.3	update or maintain risk-assessment documentation;
13.4	update or maintain risk-assessment documentation;
13.5	perform due-diligence checks on integrated components;
13.6	manage or fix vulnerabilities in integrated components;
13.7	maintain cybersecurity logs or documentation;
13.8	define support periods or run vulnerability-handling processes;
13.9	ensure long-term availability of security updates;
13.10	manage update versioning or update policies;
13.11	maintain public software repositories or issue related warnings;
13.12(1)	prepare the technical file nor conduct conformity assessment;
13.14	manage production conformity or process updates.

An authorised representative **performs the tasks specified in the mandate received** from the manufacturer.

The authorised representative **provides a copy of the mandate when** market surveillance authorities **request it**.
The **mandate** must **allow** the authorised representative **to do at least the following**:

(a) Keep documents available

The authorised representative must **keep**:
- **the EU Declaration of Conformity** (Art. 28);
- **the technical documentation** (Art. 31)

at the disposal of the market surveillance authorities for **at least 10 years after** the PDEs has been placed on the market **or for the support period**, whichever is longer.

(b) Provide information and documentation on request

If a market surveillance authority makes a **reasoned request**, the authorised representative must provide **all information and documentation necessary to demonstrate the conformity** of the PDEs.

(c) Cooperate to remove risks

The authorised representative must **cooperate with market surveillance authorities, at their request, on any action needed to eliminate the cybersecurity risks posed by the PDEs** covered by the authorised representative's mandate.

Core compliance and documentation obligations of importers - Table 1

Before placing a PDEs on the market | PDEs placed on the market | Post

19.2

Before placing a PDEs on the market, importers shall **ensure that:**

- ✅ **(a) the manufacturer has carried out the appropriate conformity assessment procedures** (Art. 32);
- ✅ **(b) the manufacturer has drawn up the technical documentation**;
- ✅ **(c) the PDEs:**
  - **1)** bears the **CE marking** (Art. 30); **and**
  - **2)** is accompanied by the **EU declaration of conformity** (Art.13.20); **and**
  - **3) is accompanied by the information and instructions to the user** set out in Annex II, in a language easily understood by users and market surveillance authorities;
- ✅ **(d) the manufacturer has complied with requirements** set out in Arts. **13(15)**,**(16)** and **(19)**.

⇨ Importers **shall be able to provide the documents** necessary to demonstrate fulfilment of these obligations.

Art. 32

Art. 30

Art. 13.20

Arts.13(15),(16),(19) Manufacturer's information obligations towards users

19.3

Where an importer **considers or has reason to believe that**:

- a **PDEs**, **or**
- the **processes** put in place by the manufacturer

⇨ **are not in conformity** with this Regulation ⟹ The importer shall **not place the PDEs on the market until** the product or the processes put in place by the manufacturer have been brought into **conformity**.

Where the PDEs presents a **significant cybersecurity risk** ⟹ The importer shall **inform**, to that effect:

- **the manufacturer and**
- **the market surveillance authorities.**

Where an importer **has reason to believe that a PDEs may present a significant cybersecurity risk in light of non-technical risk factors** ⟹ The importer shall **inform the market surveillance authorities** to that effect.

→ **Upon receipt of such information**, the market surveillance authorities shall **follow the procedures** referred to in Art. 54(2).

Art. 54.2

Core compliance and documentation obligations of importers - Table 2

PDEs placed on the market | **Post**

19.1

Importers shall **place on the market only those PDEs that:**

1) **comply with the essential cybersecurity requirements** set out in Part I of Annex I; **and**

2) **where the processes put in place by the manufacturer comply with the essential cybersecurity requirements** set out in Part II of Annex I.

Annex I, Part I | Annex I, Part II

19.5

Importers who **know or have reason to believe that a PDEs** which they have **placed on the market is not in conformity shall immediately**:

- **take the corrective measures** necessary to ensure that the PDEs is brought into conformity with this Regulation, **or**
- to **withdraw** or **recall the product, if appropriate**.

Upon becoming aware of a vulnerability in the PDEs

⇨ importers shall **inform the manufacturer without undue delay** about that vulnerability.

Where the PDEs presents a significant cybersecurity risk

⇨ importers shall **immediately inform the market surveillance authorities of the Member States** in which they have made the PDEs available on the market to that effect, **giving details**, in particular:

- of non-compliance, **and**
- of **any** corrective measures taken.

19.6

Importers shall, for **at least 10 years after the PDEs has been placed on the market or for the support period, whichever is longer,**

- **keep a copy of the EU declaration of conformity at the disposal of market surveillance authorities and**
- **ensure that the technical documentation can be made available to those authorities, upon request**.

19.7

Further to a reasoned request from a market surveillance authority

⇨ the importers **shall provide it with all information and documentation** necessary to demonstrate conformity of the PDEs with Part I and Part II of Annex I:

- in paper or electronic form;
- in a language that can be easily understood by that authority.

At its request, importers **shall cooperate with the authority, on any measures taken to eliminate cybersecurity risks posed by a PDEs** they have placed on the market.

19.8

Where the importer of a PDEs **becomes aware that the manufacturer** of that product **has ceased its operations and**, as result, **is not able to comply with the obligations** laid down in this Regulation

⇨ The importer shall **inform**

- **the relevant market surveillance authorities** about this situation,
- **as well as**, by any means available and to the extent possible, **the users** of the PDEs placed on the market.

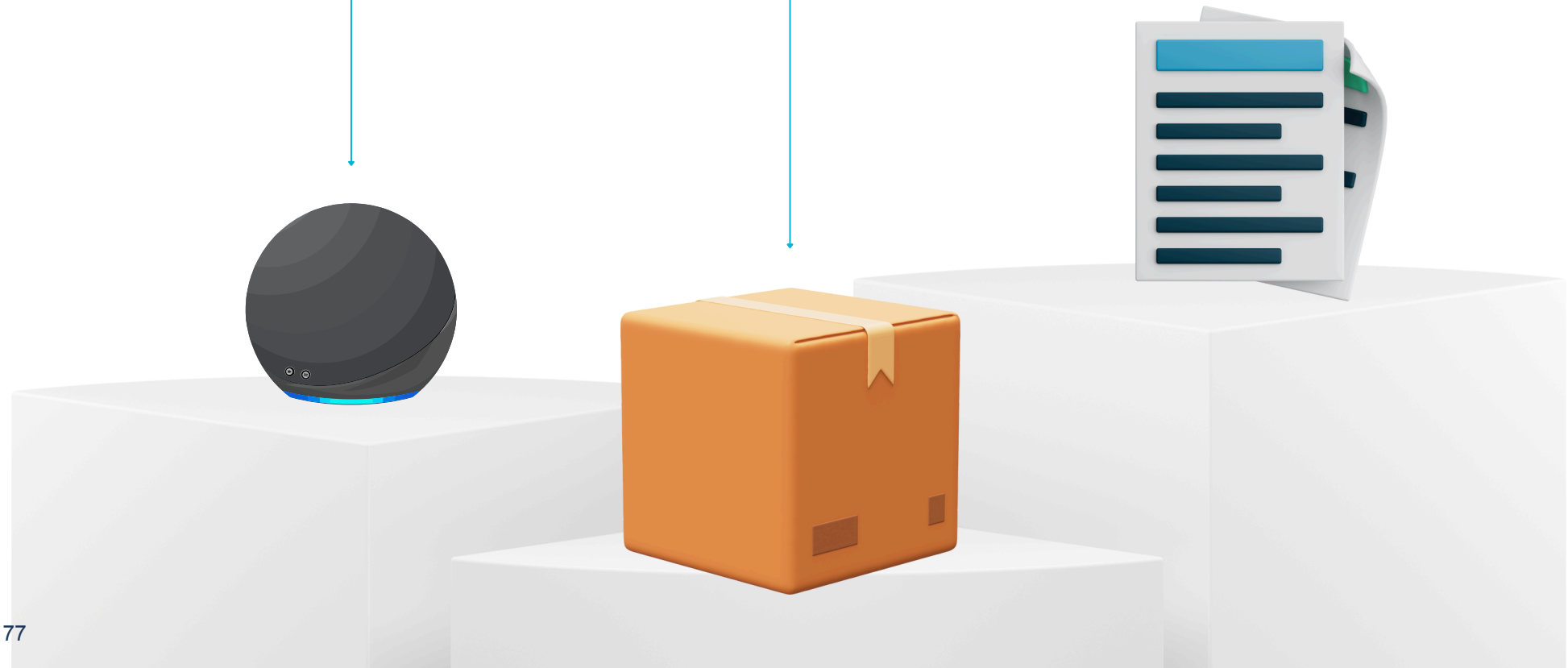
Importer's contact details

19.4

Importers **shall indicate the following on the PDEs, or on its packaging, or in a document accompanying the PDEs:**

1. **name**;
2. **registered trade name** or **registered trademark**;
3. **postal address**;
4. **email address** or other digital contact;
5. and, **where applicable**, the **website** where they can be contacted.

The contact details shall be in a **language easily understood** by **users** and **market surveillance authorities**.



Obligations of distributors - Table 1

Before placing a PDEs on the market | PDEs placed on the market | Post

20.2

Before making a PDEs available on the market, distributors shall **verify that:**

- ✅ **(a)** the PDEs bears the **CE marking**;
- ✅ **(b)** the **manufacturer and** the **importer:**
  - **have complied with the obligations** set out in Arts. **13(15)**,**(16)**,**(18)**,**(19)** and **(20)**.
  - **have complied with the obligations set out in Art. 19(4)** relating to the importer's contact details **and have provided all necessary documents** to the distributor.

Arts.13(15),(16),(19) Manufacturer's information obligations towards users

Arts.13(18) and (20) Manufacturer's information obligations towards users

Art. 19.4

20.3

❗ **Where** a distributor **considers or has reason to believe, on the basis of information in its possession, that**

- a **PDEs**, **or**
- the **processes** put in place by the manufacturer

are not in conformity with the essential cybersecurity requirements set out in Annex I ⟹ The distributor shall **not make the PDEs available on the market until** the product or the processes put in place by the manufacturer have been brought into **conformity**.

❗ **Where** the PDEs poses a **significant cybersecurity risk** ⟹ The distributor shall **inform**, **without undue delay**, to that effect:

- the **manufacturer and**
- the **market surveillance authorities**.

Obligations of distributors - Table 2

PDEs placed on the market | **Post**

20.1

When **making a PDEs available on the market,** distributors shall act with due care **in relation to the requirements** set out in this Regulation.

20.4

Distributors **who know or have reason to believe, on the basis of information in their possession**, that

- a **PDEs**, which they have made available on the market, **or**
- the **processes** put in place by its manufacturer

are not in conformity with this Regulation

⇨ **They shall make sure that**

- **the corrective measures** necessary to bring that PDEs or the processes put in place by its manufacturer into conformity **or**
- **to withdraw or recall the product, if appropriate, are taken.**

Upon becoming aware of a vulnerability in the PDEs

⇨ distributors shall **inform the manufacturer without undue delay about that vulnerability**.

Where the PDEs **presents a significant cybersecurity risk**

⇨ distributors shall **immediately inform the market surveillance authorities** of the Member States in which they have made the PDEs available on the market to that effect, **giving details**, in particular:

- of the non-compliance, **and**
- of **any** corrective measures taken.

20.5

Further to a reasoned request from a market surveillance authority

distributors shall **provide all information and documentation** necessary to demonstrate conformity of the PDEs and the processes put in place by its manufacturer with this Regulation

- in paper or electronic form;
- in a language that can be easily understood by that authority.

At its request, distributors **shall cooperate with the authority, on any measures taken to eliminate cybersecurity risks posed by a PDEs** which they have made available on the market.

20.6

Where the distributor of a PDEs **becomes aware, on the basis of information in its possession, that the manufacturer** of that product **has ceased its operations and**, as result, **is not able to comply with the obligations** laid down in this Regulation

⇨ the distributor shall **inform, without undue delay**,

- **the relevant market surveillance authorities** about this situation,
- **as well as**, by any means available and to the extent possible, **the users** of the PDEs placed on the market.

Obligations of open-source software stewards

Only to the extent it is made available on the market, that is, supplied for distribution or use in the course of a commercial activity (recital 18):

The cybersecurity policy

24.1

Open-source software **stewards shall put in place and document in a verifiable manner a cybersecurity policy** to

1) foster the **development** of a **secure** FOSS PDEs
2) as well as an **effective handling of vulnerabilities** by the developers of that product.

That policy shall:

3) **foster the voluntary reporting of vulnerabilities** as laid down in Art. 15 by the developers of that product; and
4) take into account **the specific nature** of the open-source software steward; and
5) take into account the **legal and organisational arrangements** to which it is subject.

That policy shall, in particular, include aspects related to:

6) **documenting, addressing and remediating vulnerabilities**; and
7) **promote the sharing of information** concerning discovered vulnerabilities within the open-source community.

Duty to supply documentation

24.2

Further to a reasoned request from a market surveillance authority, open-source software **stewards shall provide** that authority with the **documentation**

- in a language which can be easily understood by that authority;
- in paper or electronic form.

Art. 15
Voluntary reporting

Cooperation with market surveillance authorities

24.2

Open-source software **stewards shall cooperate with the market surveillance authorities**, **at their request**, **with a view to mitigating the cybersecurity risks posed by a PDEs** qualifying as free and open-source software.

Duty to notify actively exploited vulnerabilities and severe incidents

24.3

The obligation to notify **any actively exploited vulnerability** (Art. **14.1**) **applies** to OSS stewards **to the extent that they are involved in the development of the PDEs**.

The obligation to notify any severe incident (Art. **14.3**) and to notify **users** (Art. 14.8) **applies** to OSS stewards **to the extent that severe incidents affect network and information systems** provided by the OSS stewards for the development of such PDEs.

Art. 14.1 | Art. 14.3 | Art. 14.8

Security attestation of free and open-source software

25

To **facilitate the due diligence obligation set out in Art. 13.5**, regarding manufacturers that integrate FOSS components in their PDEs

the Commission is empowered to adopt delegated acts

by establishing voluntary security attestation programmes allowing

- **the developers**; or
- **users of PDEs** qualifying as FOSS;
- as well as **other third parties**

to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation.

26, 1 and 2(a)

To **facilitate implementation and ensure the consistency of such implementation**

the Commission shall publish guidance to assist economic operators in applying this Regulation, with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises.

Where it intends to provide guidance, **the Commission shall address at least the following aspects:**

a) **the scope** (particularly re. **remote data processing solutions and FOSS);**

b) **application of support periods;**

c) **compliance of PDEs** under the **CRA** and **other related Union legal acts;**

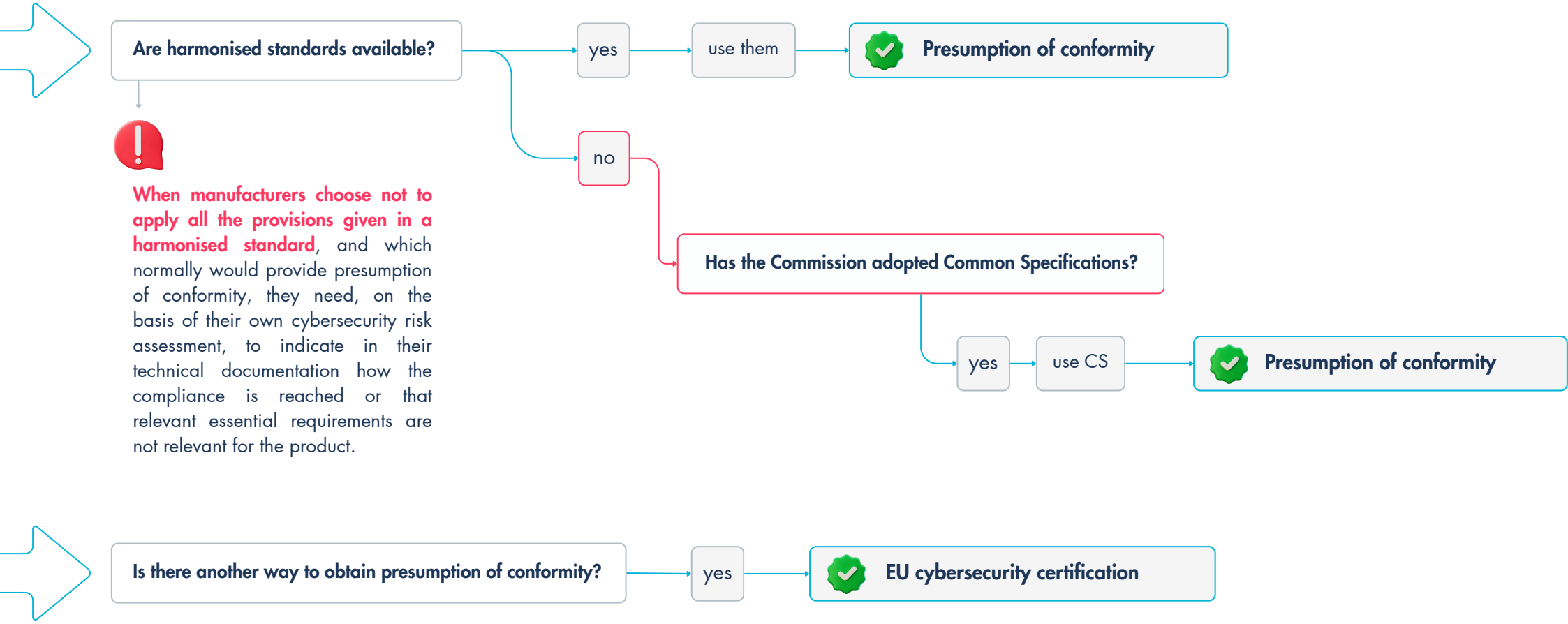
d) **concept of substantial modification**

Overview - Presumption of conformity

Under Article 6, both the **PDEs** and the **processes** put in place by the manufacturer **must comply with the essential cybersecurity requirements** set out in Annex I.
To facilitate the demonstration of compliance, **Article 27 provides several simplified conformity mechanisms**.

The **presumption of conformity is a facilitation tool, not an obligation**.

Manufacturers may still choose to demonstrate compliance by other means, **without relying** on harmonised standards or EU cybersecurity certification schemes.



When manufacturers choose not to apply all the provisions given in a harmonised standard, and which normally would provide presumption of conformity, they need, on the basis of their own cybersecurity risk assessment, to indicate in their technical documentation how the compliance is reached or that relevant essential requirements are not relevant for the product.

Presumption of conformity - Table 1

Use harmonised standards

27.1

PDEs and processes put in place by the manufacturer **which are in conformity with harmonised standards or parts thereof**, the references of which have been published in the Official Journal of the European Union, **are presumed to be in conformity** with the essential cybersecurity requirements set out in Annex I covered by those standards or parts thereof.

What if harmonised standards do not exist? **Use Common Specifications**

27.2 and 5

If harmonised standards are **not expected to be published within a reasonable period**, the Commission **may adopt implementing acts establishing common specifications** covering technical requirements that provide a means to comply with the essential cybersecurity requirements.

PDEs and processes put in place by the manufacturer **which are in conformity with the common specifications established by implementing acts are presumed to be in conformity** with the essential cybersecurity requirements set out in Annex I covered by those common specifications or parts thereof.

27.6 and 7

What happens when harmonised standards become available later?

When a reference of a **harmonised standard is published** in the Official Journal of the European Union, **the Commission shall repeal the implementing acts** or parts thereof which cover the same essential cybersecurity requirements as those covered by that harmonised standard.

What if a Member State believes a Common Specification is insufficient?

Where a Member State considers that a **common specification does not entirely satisfy the essential cybersecurity requirements** set out in Annex I, **it shall inform the Commission.** The Commission **may**, if appropriate, **amend the implementing act** establishing the common specification in question.

Presumption of conformity - Table 2

Is there **another way to obtain presumption of conformity**? Yes: **EU cybersecurity certification**

27.8 and 9

PDEs and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European Cybersecurity Certification Scheme - ECCS (Regulation (EU) 2019/881) **are presumed to be in conformity** with the essential cybersecurity requirements set out in Annex I covered by those standards.

The issuance of a certification under a ECCS with assurance level substantial or high eliminates the obligations to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), points (a) and (b), and Article 32(3), points (a) and (b).

The Commission specifies the ECCS - via delegated acts - **that can be used to demonstrate conformity of PEDs** with the essential cybersecurity requirements or parts thereof.

Art. 32.2 and 3

EU declaration of conformity - Table 1

28.1and 2

Manufacturers **draw up the EU declaration of conformity** in accordance with Art. 13.12

Art.13.12

The EU declaration of conformity shall:

1) **states that the fulfilment of the essential cybersecurity requirements** set out in Annex I **has been demonstrated**;

Annex I

2) has the **model structure** set out in **Annex V**;

3) **contains the elements specified in** the relevant conformity assessment procedures in **Annex VIII**;

Annex VIII

4) shall be made **available in the languages required by the Member State in which the PDEs is placed or made available** on the market;

5) and shall be **updated as appropriate.**

28.4

By drawing up the EU declaration of conformity, the manufacturer shall **assume responsibility for the compliance of the PDEs.**

28.3

Where a PDEs is **subject to more than one Union legal act** requiring an EU declaration of conformity

a single EU declaration of conformity shall be drawn up in respect of all such Union legal acts.

That declaration shall **contain the identification of the Union legal acts concerned**, including their publication references.

28.5

The Commission is empowered to adopt delegated acts to add elements to the minimum content of the EU declaration of conformity set out in Annex V to take account of technological developments.

ANNEX V
EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 28, shall contain all of the following information:

1. **Name and type** and any additional information enabling the unique identification **of the product with digital elements**;
2. **Manufacturer details:** name and address of the manufacturer or its authorised representative;
3. **Provider's responsibility statement:** a statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
4. **Identification of the declared object** (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate);
5. **Compliance statement:** a statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;
6. **References to** any relevant **harmonised standards** used or any other **common specification** or **cybersecurity certification** in relation to which conformity is declared;
7. Where applicable, the name and number of the **notified body**, a description of the conformity assessment procedure performed and identification of the certificate issued;

Additional information:

Signed for and on behalf of:

(**place** and **date** of issue):

(**name**, **function**) (**signature**):

Simplified EU declaration of conformity - Table 2

28.2

The **simplified** EU declaration of conformity referred to in Art. 13.20

1) has the **model structure** set out in **Annex VI**;

2) shall be made **available in the languages required by the Member State in which the PDEs is placed or made available** on the market.

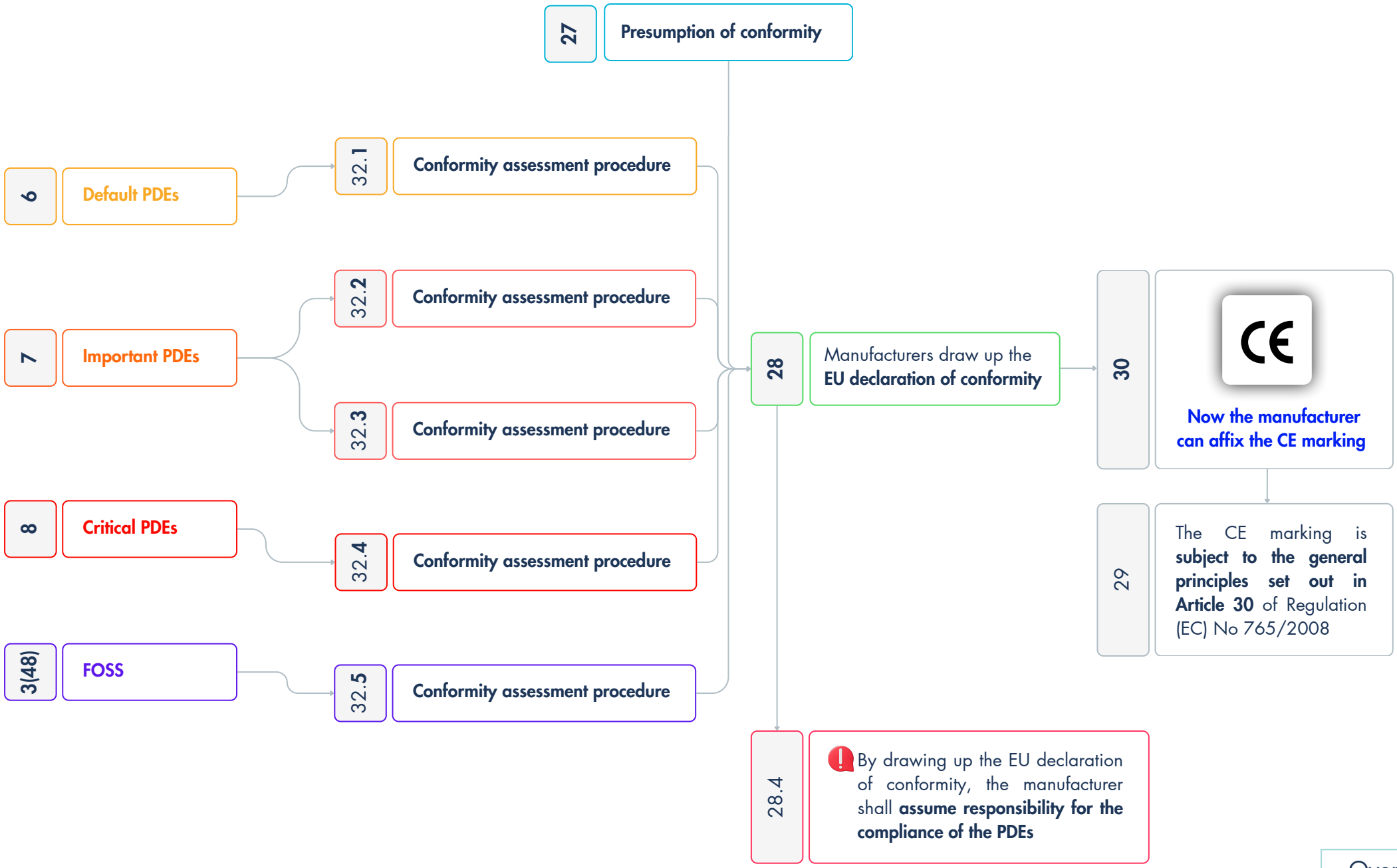
Art. 13.20

ANNEX VI
SIMPLIFIED EU DECLARATION OF CONFORMITY

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

Hereby, … [name of manufacturer] declares that the product with digital elements type … [designation of type of product with digital element] is in compliance with Regulation (EU) 2024/2847.
The full text of the EU declaration of conformity is available at the following internet address: …

Overview - EU declaration of conformity



Rules and conditions for affixing the CE marking - Table 1

32 Manufacturers **carry out the chosen conformity assessment procedure.**

28 **Manufacturers shall draw up the EU declaration of conformity** in accordance with Art. 28.

29 **and affix the CE marking, which is subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.**

Before placing a PDEs on the market | PDEs placed on the market | Post

30.1-2 and 3

The CE marking shall be:

1) affixed **before** the PDEs is placed on the market;
2) It **may** be **followed by a pictogram or any other mark indicating a special cybersecurity risk or use** set out in the implementing acts referred to in Art. 30.6;
3) **affixed visibly, legibly and indelibly** to the PDE;

Where that is not possible or not warranted on account of the **nature** of the PDEs, it shall be **affixed**

- **to the packaging**, **and**
- **to the EU declaration of conformity** (Art. 28) accompanying the PDEs.

Software:

For PDEs which are in the form of **software**, the CE marking shall be **affixed either**

- **to the EU declaration of conformity** (Art. 28), **or**
- **on the website** accompanying the software product.
  In the latter case, the relevant section of the website shall be **easily and directly accessible to consumers**.

On account of the **nature of the PDEs**:

- the **height of the CE marking** affixed to the PDEs **may** be **lower than 5 mm**, **provided that it remains visible and legible**.

Art. 30.6 | Art. 28

Rules and conditions for affixing the CE marking - Table 2

30.4

Where a notified body is involved in the conformity assessment procedure based on full quality assurance (module H - Art. 32).

⇨ CE **The CE marking shall be followed by the identification number of that body.**

The identification number of the notified body shall be **affixed**

- **by the body itself; or**
- **under its instructions, by the manufacturer or the manufacturer's authorised representative.**

30.5

Member States shall

- **build upon existing mechanisms** to ensure correct application of the regime governing the CE marking, **and**
- **shall take appropriate action in the event of improper use of that marking**.

Where the PDEs is subject to Union harmonisation legislation, other than the CRA, **which also provides for the affixing of the CE marking**

⇨ CE The CE marking **shall indicate that the product also fulfils the requirements** set out in such other Union harmonisation legislation.

30.6

The Commission may, by means of implementing acts, lay down technical specifications for

- labels;
- pictograms;
- or any other marks related to the security of the PDEs;
- their support periods;
- and mechanisms to promote their use and to increase public awareness about the security of PDEs.

When preparing the draft implementing acts, **the Commission shall consult relevant stakeholders.**

Technical documentation

Before placing a PDEs on the market | PDEs placed on the market | Support period

31.2

The technical documentation shall be

- **drawn up before the PDEs is placed on the market,** and
- **continuously updated,** where appropriate, **at least during the support period.**

31.1

The technical documentation shall

- **contain all relevant data or details of the means used by the manufacturer to ensure that the PDEs and the processes** put in place by the manufacturer **comply** with the essential cybersecurity requirements set out in Annex I;

It shall at least contain the elements set out in Annex VII

31.5

The Commission is empowered to adopt delegated acts by **adding elements to be included in the technical documentation set out in Annex VII** to take account of technological developments, as well as developments encountered in the implementation process of this Regulation.

31.4

The technical documentation **and** correspondence relating to **any conformity assessment procedure** shall be drawn up

- **in an official language of the Member State in which the notified body is established or**
- **in a language acceptable** to that body.

31.3

For **PDEs** as referred to in Art. **12**, **which are also subject to other Union legal acts which provide for technical documentation,**

⇨ **a single set of technical documentation shall be drawn up** containing the information referred to in Annex VII **and** the information required by those Union legal acts.

Art. 12

Choosing the conformity procedure - Default and Important PDEs

Depending on the classification of the product, **the manufacturer demonstrates conformity with the essential cybersecurity requirements by using the following procedures:**

Annex VIII

Default PDE

32.1

For all default PDEs, **the manufacturer is free to choose any** of the following **4** conformity assessment procedures:

Procedure type:

(a) **Module A** (self-assessment) **Internal control procedure** (Annex VIII, Part **I**)

(b) **Modules B + C** **EU-type examination** (B) and **internal production control** (C) (Annex VIII, Parts **II–III**)

(c) **Module H** **Full quality assurance** (Annex VIII, Parts **IV**)

(d) **Where available and applicable** **European cybersecurity certification scheme** (Article 27.9)

Important PDE - Class I

32.2

- **Where** the manufacturer has **not applied or has only partly applied**, harmonised standards, common specifications, or a European cybersecurity certification scheme at assurance level **at least** "**substantial**";
- **or where such** standards, specifications or certification schemes **do not exist,**

then the manufacturer **must undergo conformity assessment involving a third-party**:

(a) **Modules B + C** **EU-type examination** (B) followed by **internal production control** (C) (Annex VIII, Parts **II–III**)

(b) **Module H** **Full quality assurance** (Annex VIII, Parts **IV**)

Key term: **harmonised standard**

Important PDE - Class II

32.3

For Class II important products, **the conformity assessment must always involve a third-party:**

(a) **Modules B + C** **EU-type examination** (B) followed by **internal production control** (C) (Annex VIII, Parts **II–III**)

(b) **Module H** **Full quality assurance** (Annex VIII, Parts **IV**)

(c) **Where available and applicable** **European cybersecurity certification scheme** at assurance level **at least** '**substantial**' (Article 27.9)

Critical PDE

32.4

The manufacturer demonstrates conformity with the essential cybersecurity requirements by using **one of the following 2 procedures**:

(a) Obtaining a **European cybersecurity certification** in accordance with **Article 8.1**

→ **Article 8.1 grants the Commission the power to adopt delegated acts** that can make European cybersecurity certification (ECCS) **mandatory** for certain categories of critical PDEs.

To activate the certification requirement under Article 8.1, all of the following conditions must be met:

1. **An EU cybersecurity certification scheme exists** and it must have been adopted under the Cybersecurity Act (Regulation EU 2019/881).
2. The **scheme covers the critical products listed in Annex IV**;
3. The Commission has adopted a **delegated act mandating the use of that scheme** for those products;
4. The delegated act **specifies the required assurance level**, which must be **at least** "**substantial**" and **proportionate** **to the cybersecurity risk** associated with the product.

→ Art. 8

(b) **Where no delegated acts are adopted, the manufacturer must follow any of the procedures in Article 32(3)** (Modules B + C or H):

→ **Modules B + C**
EU-type examination (B) followed by **internal production control** (C) (Annex VIII, Parts **II–III**)

→ **Module H**
Full quality assurance (Annex VIII, Parts **IV**)

→ **Where available and applicable**
European cybersecurity certification scheme at assurance level **at least** '**substantial**' (Article 27(9))

FOSS PDE

32.5

Manufacturers of products that qualify as **free and open-source software** and **fall under the categories of Annex III (i.e. Important PDEs)** demonstrate conformity by using **one** of the procedures:

(a) **Module A** (self-assessment)
Internal control procedure
(Annex VIII, Part **I**)

(b) **Modules B + C**
EU-type examination (B) and **internal production control** (C)
(Annex VIII, Parts **II–III**)

(c) **Module H**
Full quality assurance
(Annex VIII, Parts **IV**)

(d) **Where available and applicable**
European cybersecurity certification scheme
(Article 27(9))

In all cases, the technical documentation referred to in Article 31 must be made publicly available at the time of the placing on the market of those products.

Overview - Type of assessment

Depending on the classification of the product and the application of harmonised standards or certification,
the manufacturer demonstrates conformity with the essential cybersecurity requirements by using one of the following procedures:

Procedures	Type of assessment	Made by	Effect
Module A	Conformity based on **internal control**	**Manufacturer** **No notified bodies**	The **manufacturer** 1. **verifies** that the PDEs complies with the essential requirements of the CRA; **and** 2. **declares** compliance under **its sole responsibility**.
Module B+C	**EU-type examination**	**Manufacturer** **Notified bodies**	1. The **manufacturer verifies** that the PDEs complies with the essential requirements of the CRA; 2. a **notified body examines** the design and development of the product; **and** 3. the **manufacturer declares** compliance.
Module B+C	Conformity based on **full quality assurance**	**Manufacturer** **Notified bodies**	1. The **manufacturer implements a full quality control system** that ensures that the products subject to this system comply with the essential requirements of the CRA in both the design and the production phases; 2. a **notified body assesses** the overall performance of the quality control system, including periodical tests and checks; 3. The **manufacturer declares** compliance with the CRA requirements before placing the products on the market.

Module A

Procedures	Type of assessment	Made by	Effect
Module A	Conformity based on **internal control**	**Manufacturer** **No notified bodies**	The **manufacturer** 1. **verifies** that the PDEs complies with the essential requirements of the CRA; **and** 2. **declares** compliance on **its sole responsibility**.

Products

The following categories of products are allowed to use module A:

- **Default category: all PDEs that do not have the core functionality of a category of important or critical products;**
- **Important PDEs of class I, if harmonised standards have been applied** in accordance with Article 32(2);
- **Important PDEs of class I or II, if they are FOSS provided that the technical documentation is made available to the public**, in accordance with Article 32(5).

Activities

The manufacturer has to perform the following **activities**:

1) **Implement the necessary cybersecurity mitigation measures** in the product following the risk assessment;
2) **Verify** (via testing or other mechanism) **that the product complies to the relevant essential requirements of the CRA**;
3) **Draw up the technical documentation**;
4) Where the manufacturer can demonstrate that the PDEs complies with the essential requirements, **affix the CE marking, draw up and sign a declaration of conformity**;
5) **Ensure that the production of the different units of the PDEs does not alter the compliance with the CRA essential requirements**.

Module B+C - Table 1

Procedures	Type of assessment	Made by	Effect
Module B+C	EU-type examination	Manufacturer Notified bodies	1. The **manufacturer verifies** that the PDEs complies with the essential requirements of the CRA; 2. a **notified body examines** the design and development of the product; **and** 3. the **manufacturer declares** compliance.

Products

The manufacturer can undertake a conformity assessment procedure based on module B+C **for all categories of products covered by the CRA.**

Module B+C or H are mandatory in the following cases:

- **Important PDEs of class I if harmonised standards have not been applied (or only in part)**, in accordance with Article 32(2);
- **Important products of class II**;
- **Critical products** [**unless the use of a European cybersecurity certification scheme is made mandatory in the future** in accordance with Article 8(1].

Module B+C - Table 2

Activities

The manufacturer and the notified body have to perform **the following activities**:

The manufacturer

1) **implements the necessary cybersecurity mitigation measures** in the product following the risk assessment;
2) **tests the product** in order to verify that it complies with the relevant essential requirements of the CRA;
3) **draws up the technical documentation**;
4) The notified body **assesses the design of the product**, based on its technical documentation, **and one specimen or sample**.

   The notified body **does not only carry out a documentation-based assessment, but it additionally performs the necessary tests**, either itself or via an external laboratory. The manufacturer might need to be involved in those tests.

   Once the notified body concludes that the product is compliant with the CRA, it issues an EU-type certificate, which is **valid for a certain period of time**, as defined by the notified body.

5) **Once** the manufacturer **obtains the EU-type certificate, it affixes the CE marking (together with NANDO number of the body), draws up and signs a declaration of conformity**;
6) **The manufacturer ensures that the production of the different units of the product does not alter the compliance with the CRA essential requirements,** as laid down in point 2 of module C.

Only one notified body participates in this procedure and examines the whole product and all relevant essential requirements.

The production phase is not assessed by the notified body. In other words, the manufacturer **cannot justify** that a product whose design is compliant with the CRA is not, in the practice, compliant because of a defect in the production process.

Substantial modifications of the product require a new assessment by the same or a different notified body, that might lead to a potential revision of the issued EU-type certificate.
Other modifications that do not affect the compliance with the CRA requirements **are not subject to reassessment** by the notified body.

In accordance with point 8 of module B, **the notified body must carry out periodic audits to ensure that the vulnerability handing processes are properly implemented**.

Information about EU-type certificates and their revisions has to be shared with other notified bodies and with the notifying authorities, according to point 9 of module B.

Module H - Table 1

Procedures	Type of assessment	Made by	Effect
Module B+C	Conformity based on **full quality assurance**	**Manufacturer** **Notified bodies**	1. The **manufacturer** **implements a full quality control system** that ensures that the products subject to this system comply with the essential requirements of the CRA in both the design and the production phases; 2. a **notified body** **assesses** the overall performance of the quality control system, including periodical tests and checks; 3. The **manufacturer** **declares** compliance with the CRA requirements before placing the products on the market.

Products

This module might be **particularly considered by manufacturers** that place

- **numerous product types on the market or**
- **products subject to frequent updates,**

since it streamlines the relevant conformity assessment procedures for each new or substantially modified product.

Module H might be helpful for manufacturers of important and critical products that place numerous types or models on the market since it provides a **holistic system** that streamlines the conformity assessment.

Module H - Table 2

Activities

The manufacturer and the notified body have to perform **the following activities**:

1) The manufacturer **implements a full quality control system that covers**

- a **certain catalogue of products** and
- **all the relevant manufacturing phases**, from design to production;

The system can be based on international standards (for example, ISO 9000 series covering the specificities of the CRA).
The fact that the manufacturer is accredited against the standard ISO 9000 does not automatically entitle it to perform conformity assessment activities under module H, since the involvement of a CRA notified body is needed.

2) The notified body **assesses the quality control system as a whole, including, among others,**

1. the technical design of the covered products,
2. the standards or specifications to be applied (in particular, how the compliance with the essential requirements of the CRA is ensured),
3. the tests to be performed, and
4. the monitoring of the overall system.

The notified body **covers the whole manufacturing process**.

The manufacturer, **based on the quality control system,**

3) **implements the necessary cybersecurity mitigation measures** in the PDEs following the risk assessment;
4) **tests the product** in order to verify that it complies with the relevant essential requirements of the CRA;
5) **draws up the technical documentation**;
6) **affixes the CE marking (together with the NANDO number of the notified body)**;
7) **draws up and signs a declaration of conformity**;
8) **ensures that the production of the different units of the product does not alter the compliance with the CRA essential requirements**.

Only one notified body participates in this procedure and examines the whole quality control system.

The manufacturer can extend the scope of the described quality system to new or substantially modified products.
The quality system must be updated in order to properly document the new scope, and potential new standards might need to be applied or tests might need to be performed. Nevertheless, **this extension is subject to a new assessment by the same notified body that performed the original assessment**.
Module H provides a more versatile and flexible framework compared to module B+C. Hence, the inclusion of new products constitutes a more streamlined process, **since the notified body will only have to assess the potential new standards or tests applicable to the new products**.

64.2

Non-compliance with

- **the essential cybersecurity requirements** set out in **Annex I**; and
- **the obligations** set out in Arts. **13** and **14**

⇨ shall be subject to **administrative fines** of up to **EUR 15 000 000**

OR → if the offender is an undertaking, **up to 2,5 %** of the its total worldwide annual turnover for the preceding financial year, **whichever is higher**.

64.3

Non-compliance with the obligations set out in

- **Arts. 18 to 23**: obligations of other economic operators other than the manufacturer;
- Art. **28**: EU declaration of conformity;
- Art. **30(1) to (4)**: rules concerning the CE marking;
- Art. **31(1) to (4)**: technical documentation;
- Art. **32(1), (2) and (3)**: conformity assessment procedures;
- Art. **33(5)**: simplified technical documentation for microenterprises and small enterprises, including start-ups;
- Art. **39**: notified bodies requirements;
- Art. **41**: subsidiaries of and subcontracting by notified bodies;
- Art. **47**: operational obligations of notified bodies;
- Art. **49**: information obligations of notified bodies;
- Art. **53**: granting Market Surveillance Authorities access to data and documentation.

⇨ shall be subject to **administrative fines** of up to **EUR 10 000 000**

OR → if the offender is an undertaking, **up to 2 %** of its total worldwide annual turnover for the preceding financial year, **whichever is higher**.

64.4

The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities **in reply to a request**

⇨ shall be subject to **administrative fines** of up to **EUR 5 000 000**

OR → if the offender is an undertaking, **up to 1 %** of its total worldwide annual turnover for the preceding financial year, **whichever is higher**.

64.9

Administrative fines may be imposed, depending on the circumstances of each individual case, **in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.**

64.10

By way of derogation from paragraphs 3 to 9

The administrative fines shall not apply to the following:

(a) manufacturers that qualify as **microenterprises or small enterprises** with regard to **any** failure to meet the deadline referred to in Art. **14.2, point (a), or** Art. **14(4), point (a)**;

(b) **any infringement of this Regulation by open-source software stewards.**

Art. 14

64.1

Member States shall

- **lay down the rules on penalties applicable to infringements of this Regulation**, and
- **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 **measures**.

and shall notify it, without delay, of **any subsequent amendment** affecting them.

64.8

Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies.

The application of such rules in those Member States shall have an **equivalent effect**.

64.5

When **deciding on the amount of the administrative fine in each individual case**, **all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:**

(a) the nature, gravity and duration of the **infringement** and of **its consequences**;

(b) whether **administrative fines have been already applied** by the same or other market surveillance authorities to the same economic operator for a **similar infringement**;

(c) the **size**, in particular with regard to microenterprises and small and medium sized-enterprises, including start-ups, and the market share of the economic operator committing the infringement.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE