Vulnir

Deep Dive Session Security Controls – 40000-1-4

05 th March 2025

Angelo D'Amato
Founder

Meet your speaker

Angelo D'Amato
Founder / Cybersecurity Expert, Vulnir

Background

- With over fifteen years of experience, he is the subject matter expert for:
  - End-to-end cybersecurity assessments (Penetration testing, Security assessments)
  - Certifications and assessment (e.g., EN 303 645, Common Criteria, IEC 62443)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur as a CEN contractor (*) within CEN/CLC/JTC 13/WG 9 for the following CRA standards:
  - PT2: Generic Security Requirements (prEN 40000-1-4)
  - PT3: Vulnerability handling requirements (prEN 40000-1-3)

* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

CEN CENELEC EFTA European Commission

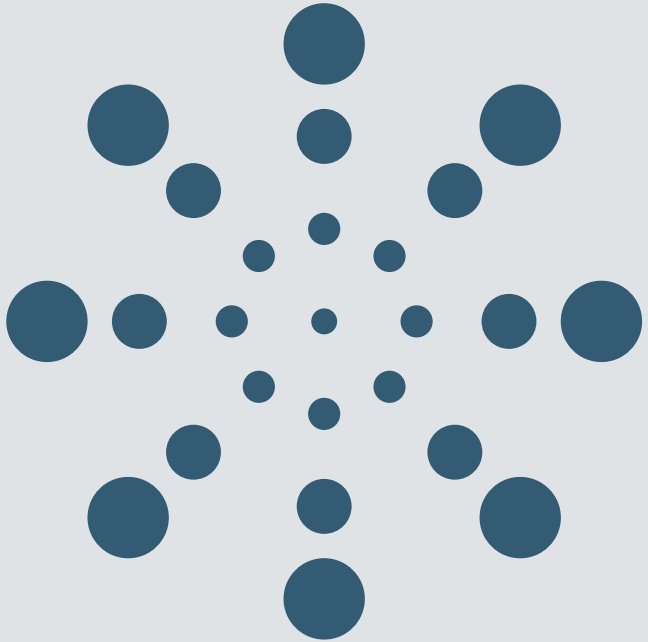
Vulnir

Agenda

01

Setting up the context

Preliminary knowledge



How and where to learn more?

- Cyber Resilience Act: Standardization Request Officially Accepted by CEN, CENELEC, and ETSI
  - Including:
    - CEN, CENELEC and ETSI Work Programme
    - WG9 convener Ben Kokx – Youtube Video
- **Core knowledge:**
  - Cyber Resilience Act - Legal Text - Regulation (EU) 2024/2847
  - Make sure that you are familiar with the CRA-related C(2025)618 – Standardisation request M/606
- **To have a better understanding and contextualization:**
  - New legislative framework
  - The Blue Guide on the implementation of the product rules 2022
  - Cyber Resilience Act - Impact assessment (REPORT / STUDY Publication 15 September 2022)

Latest updates (as per March 2026)

- **STAN4CR –** The STAN4CRA Projects, comprising STAN4CR and STAN4CR2, are European initiatives funded by the European Innovation Council and SMEs Executive Agency (EISMEA) and EFTA.
- **Cyber Resilience Act – Implementation –** Official Portal on CRA from the European Commission where you can find:
  - Official Frequently Asked Questions on CRA Implementation
  - Implementation Act on technical description related to important and critical products
- **ENISA:**
  - Single Reporting Platform (SRP) - ENISA launched a new webpage with frequently asked questions on reporting obligations and the development of the Single Reporting Platform
- **European Commission:**
  - **Draft Commission guidance on the Cyber Resilience Act (LINK)**
    - Draft Act Feedback period 03 March 2026 - 31 March 2026

Obligations of manufacturers (CRA)

Risk Assessment

Product-related essential requirements

Vulnerability handling essential requirements

Conformity assessment

Article 13

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

2. For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

Vulnerability handling throughout the product lifetime (for the period when the product is expected to be in use)

Design and development

Maintenance

Obligation to report through a single reporting platform:
(1) actively exploited vulnerabilities
(2) severe incidents having an impact on the security of the product

Reporting obligations

Source: CEN/CENELEC Webinar on 10 March 2025 – Standardisation for the Cyber Resilience Act

Article 6 - Requirements for products with digital elements

Products with digital elements 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.**

CEN-CLC JTC 13 Cybersecurity and Data Protection
WG9 / WG6

EN 40000-1-1 Vocabulary	**EN 40000-1-2** Principles for Cybersecurity	TOPIC 40
EN 40000-1-3 Vulnerability Handling	**EN 40000-1-4** Generic security requirements	

CLC TC 47 X Semiconductors and Trusted Chips Implementation	TOPIC 37-38 TOPIC 28-29 TOPIC 41
CEN TC 224 Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	TOPIC 16 TOPIC 41 TOPIC 39
CENELEC TC 65X Industrial-process measurement, control and automation	TOPIC 20-22 TOPIC 25 TOPIC 27 TOPIC 36

ETSI Technical Committee on Cyber Security

EN 304 617 Browsers	**EN 304 621** Network Management System	**EN 304 625** Virtual Network Interfaces	**EN 304 631** Smart home assistants	**EN 304 636** Firewall
EN 304 618 Password Managers	**EN 304 622** SIEM Systems	**EN 304 626** Operating Systems	**EN 304 633** Internet connected toys	**EN 304 642** Network function telecom
EN 304 619 Antivirus	**EN 304 623** Boot Managers	**EN 304 627** Routers, modem and switches	**EN 304 634** Personal wearables	
EN 304 620 VPN	**EN 304 624** PKI	**EN 304 632** Smart home security products	**EN 304 635** Hypervisors	

***Source**: C(2025)618 – Standardisation request M/606 – LINK*

Interplay between horizontal standards

EN 40000-1-2 (Project 1)
High level process **activities** to address the Total Product Life Cycle, defining:
- Goal that needs to be achieved
- Mandatory and optional inputs
- Minimum expected outcomes

Process activities such as security monitoring, risk assessment, verification, validation and release

EN 40000-1-3 (Project 3)
More detailed process **activities** (with assessment criteria fit for a presumption of conformity) to address the vulnerability management requirements

During risk assessment the appropriate security controls and their appropriate level can be selected to ensure risks are mitigated to an acceptable level

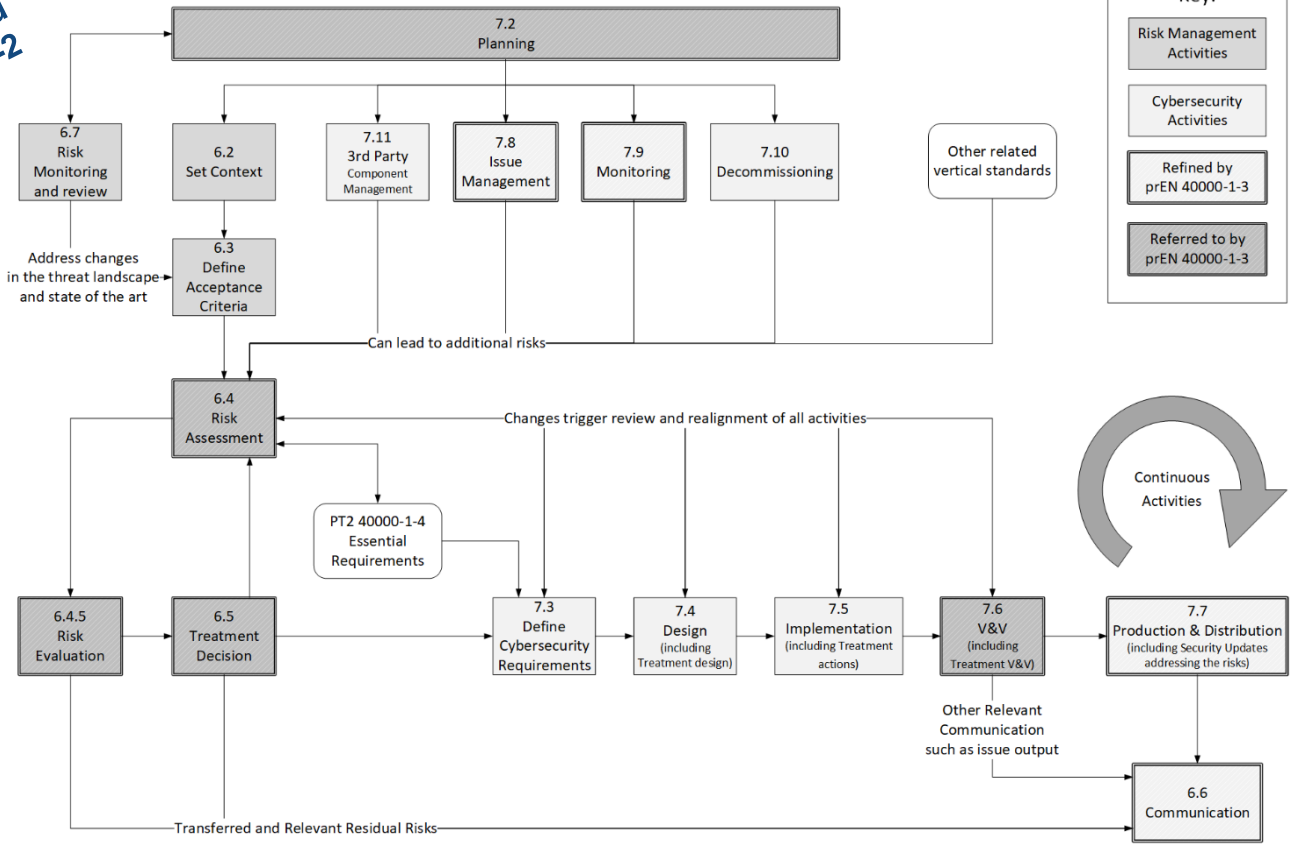
Risk assessment

Elicit requirements

EN 40000-1-4 (Project 2)
A mapping of the essential product requirements to a list of appropriate **security controls** at various levels (controls have their own scale/levels to achieve the goal of the security control)

During the elicit requirements activity the deliverables from project 2 can be used to determine and select the appropriate security controls that should be implemented into the product to fulfil on a risk-based manor the essential requirements

DRAFT PROPOSAL for an Informative Annex Showing relationships between standards and clause of the 40000-1-2

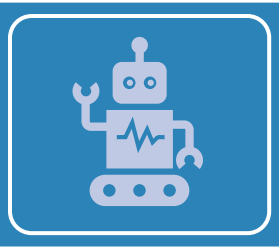


NOTE – This slide was created by WG9 experts for informational purposes and is subject to change and further refinement.

Main objectives of the deliverables

EN 40000-1-2: Principles for cyber resilience

- Covers CRA Annex I, Part 1, Requirement 1
- **Process** standard to ensure products are developed and maintained with a risk-based approach to cover **any** security risks (as a catch-all, as 2a-m do not cover all possible cybersecurity risks)
- Implementation demonstrated via documented process outputs



EN 40000-1-4: Generic security requirements

- Covers CRA Annex I, Part 1, Requirement 2 (a-m)
- **Product** standard addressing a specific set of security requirements by mapping security objectives to a catalog of possible security controls
- Implementation demonstrated via the product itself and/or supported by technical documentation

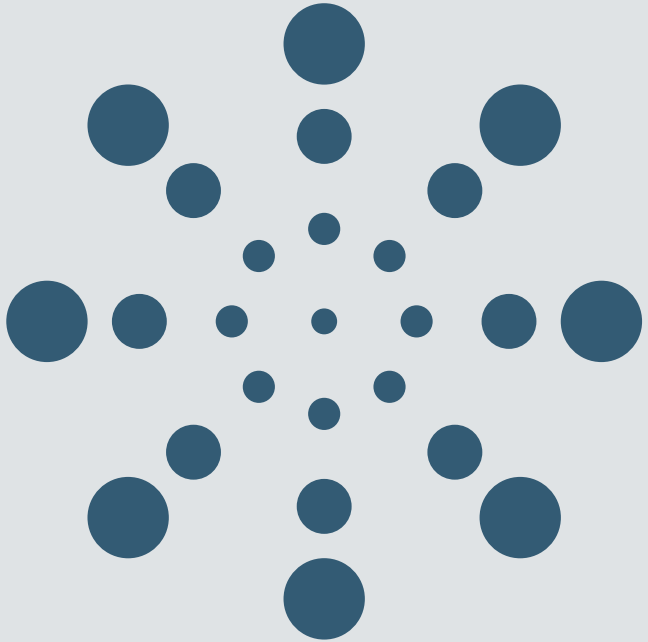
EN 40000-1-3: Vulnerability handling

- Covers CRA Annex I, Part 2
- **Process** standard to ensure products are maintained in a secure state using a risk-based approach
- Implementation demonstrated via documented process outputs and actions in the market (updates, notifications, recalls, etc.)

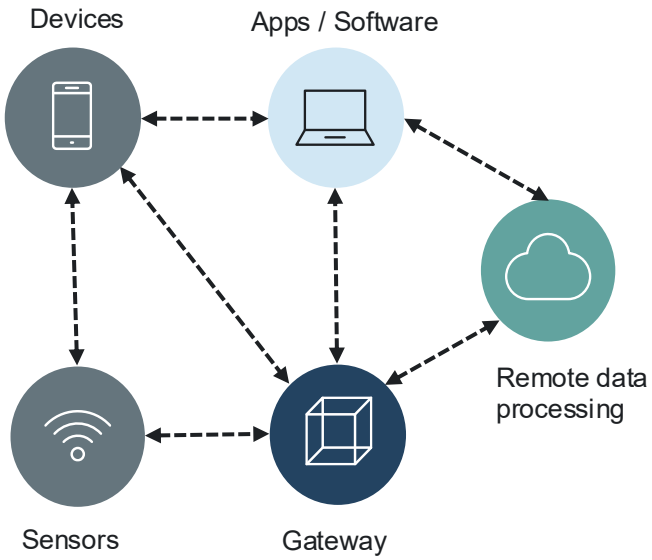
02

Essential Requirements

Understanding of the essential requirements and relevant Product security related extract/recitals from the CRA's text



Overview of the CRA's Essential Requirements



(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;

- Ensure that products with digital elements **hardware and software** placed on the EU market **have fewer cybersecurity vulnerabilities**.
- **Better protection** for consumers, supply chains, organisations, businesses, and IT Infrastructure

- **Secure by Design / Risk Assessment**
  - No known exploitable vulnerabilities
  - Secure by default configuration
  - Security updates
  - Authorized access
  - Confidentiality protection
  - Integrity protection
  - Data minimization
  - Availability protection
  - Minimize negative impact
  - Attack surface minimization
  - Reduce the impact of an incident
  - Logging and monitoring controls
  - Secure deletion mechanisms
- **Vulnerability Handling Requirements**

Essential Requirements ANNEX I PART II Vulnerability Handling

- Ensure that products with digital elements **hardware and software** placed on the EU market **have fewer cybersecurity vulnerabilities**.
- **Better protection** for consumers, supply chains, organisations, businesses, and IT Infrastructure

- **Secure by Design / Risk Assessment**
- **Vulnerability Handling Requirements**

- Identify vulnerabilities / SBOM
- Remediate vulnerabilities
- Regular test
- Inform on fixed vulnerabilities
- CVD Policy in place
- Intake of potential vulnerabilities
- Secure distribution of updates
- Update available and related dissemination

C(2025)618 – Standardisation request M/606

(6) Taking into account the broad scope of the Cyber Resilience Act, a two-fold approach for developing the standards in response to this request is appropriate. On the one hand, a set of horizontal standards should provide a coherent generic framework, methodology and taxonomy that can be used to develop further product-specific standards responding to market needs. On the other hand, certain vertical standards are needed, notably as regards the products listed in Annex III of the Cyber Resilience Act, covering a specific set of risks appropriate to a particular intended purpose and reasonably foreseeable use.

(25) Without prejudice to needed improvements, CEN, Cenelec and ETSI should take into account, as appropriate, the standardisation work carried out in the context of Commission Implementing Decision (EU) 2023/2444,[10] Regulation (EU) 2024/1689, and also forthcoming standardisation requests such as for Directive 2006/42/EC of the European Parliament and of the Council, and Regulation (EU) 2023/1230, in the preparation and development of the requested harmonised European standards. CEN, Cenelec and ETSI should also consider any other relevant on-going European standardisation activities related to other Union legislation, such as Regulation (EU) 2023/1781.

[10] COMMISSION IMPLEMENTING DECISION on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30

EUROPEAN COMMISSION

Brussels, 3.2.2025
C(2025) 618 final

COMMISSION IMPLEMENTING DECISION

of 3.2.2025

on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(only the English, French and German texts are authentic)

NOTE – EN 18031-X:2024 was built using the IEC 62443-4-2 and ETSI EN 303 645 as the main inputs!

Source: Standardisation request M/606 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/606_en

C(2025)618 – Standardisation request M/606

Coherence

The harmonised standards developed in response to this request should build on the wo currently under development to support Commission Delegated Regulation (EU) 2022/30 without prejudice to needed improvements. The specificities of Regulation (EU) 2024/284 shall however be fully addressed during the development stage. Where possible, CE Cenelec and ETSI may update already existing standards and standardisation deliverables align with the requirements of the Cyber Resilience Act.

NOTE: Starting as a baseline from:

- **EN 18031-1:2024:** Part 1: Internet-connected radio equipment
- **EN 18031-2:2024:** Part 2: radio equipment processing data, namely Internet-connected radio equipment, childcare radio equipment, toys radio equipment, and wearable radio equipment
- **EN 18031-3:2024:** Part 3: Internet-connected radio equipment processing virtual money or monetary value

It is a more concrete way to think of achieving coherence considering the following timeline:

- Horizontal standards
  - EN 40000-1-2 / EN 40000-1-3 as of 30/08/2026
  - EN 40000-1-4 as of 30/10/2027
- Vertical standards to be delivered by 30/10/2026

Brussels, 3.2.2025
C(2025) 618 final

ANNEXES 1 to 2

ANNEXES

to the

Commission Implementing Decision

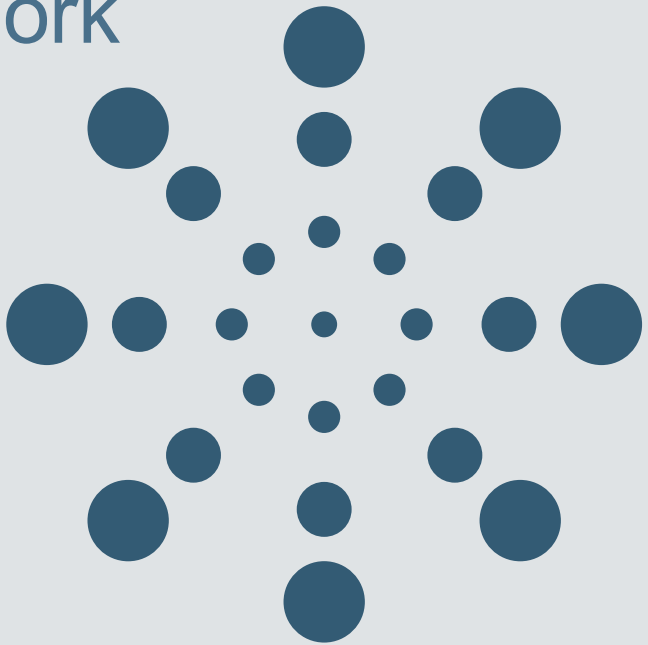
on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

Source: Standardisation request M/606 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/606_en

03

Security Controls Framework

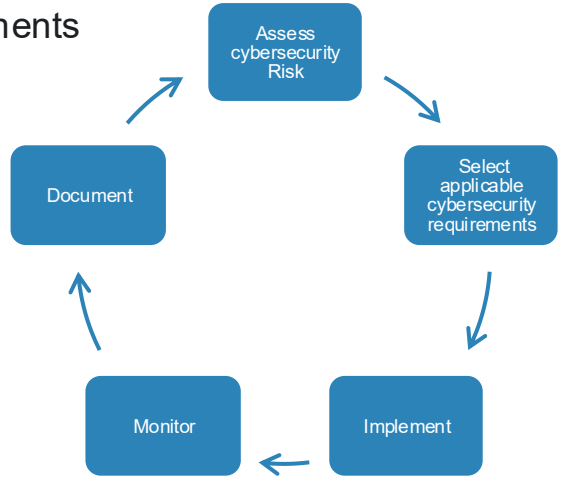
Prepare

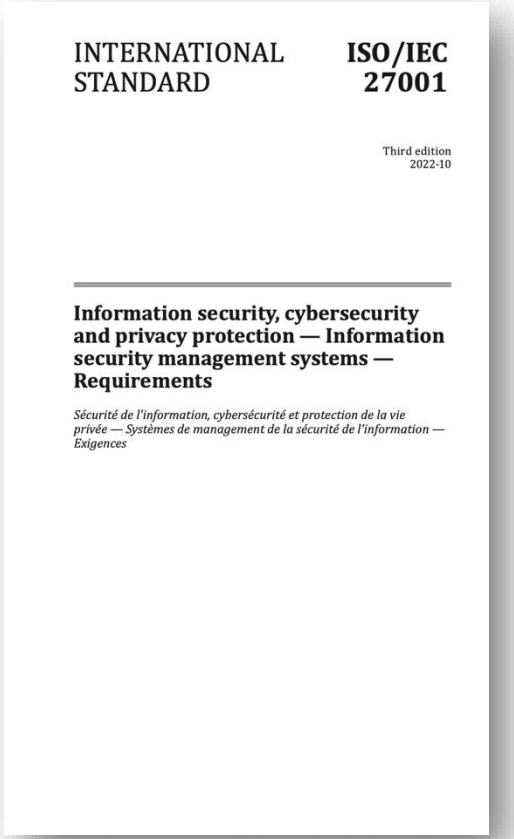


ISMS

ISO 27001 is a security standard that helps protect information assets by establishing an information security management system

- Identifying information security requirements
- Assessing information security risks
- Treating information security risks
- Selecting and implementing controls
- Monitor, maintain, and improve the effectiveness of the ISMS
- Continual improvement




INTERNATIONAL STANDARD

ISO/IEC 27001

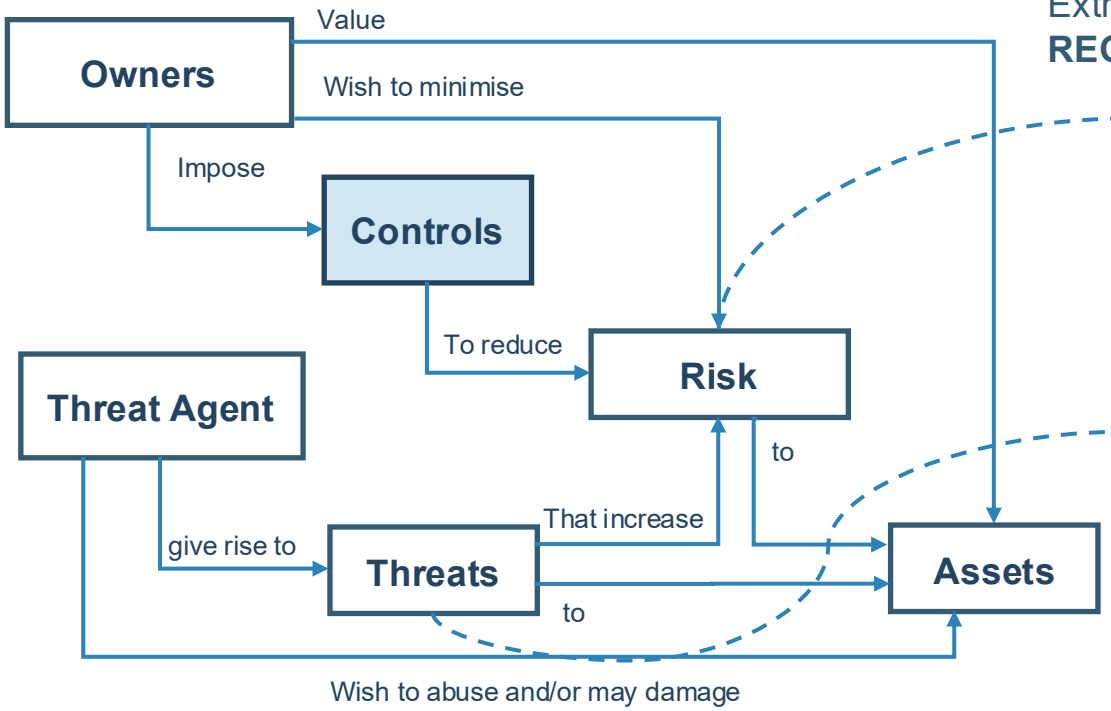
Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

***Source**: Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis*

Security concepts and relationships



Extract from:
REGULATION (EU) 2024/2847 (CRA)

- (37) '**cybersecurity risk**' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

….

- (46) **'Cyber threat'** means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

….

***Source**: CC:2022 Part 1: Introduction and general model (CCMB-2022-11-001) – Page 37 - Figure 1 — Security concepts and relationships*

Example of security frameworks

ETSI TS 103 305-1 V5.1.1 (2025-09)

Cyber Security (CYBER);
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls

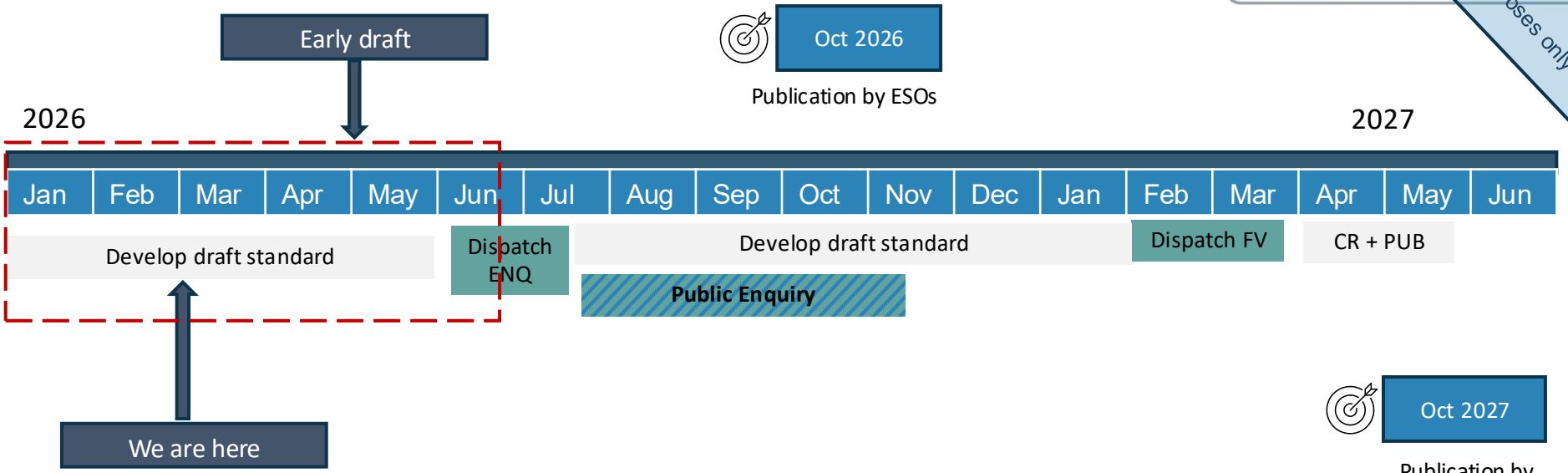
ETSI TS 104 219 V0.0.7 (2026-01)

Cyber Security (CYBER);
Software Security Development
and Implementation Framework

PT2 Objectives

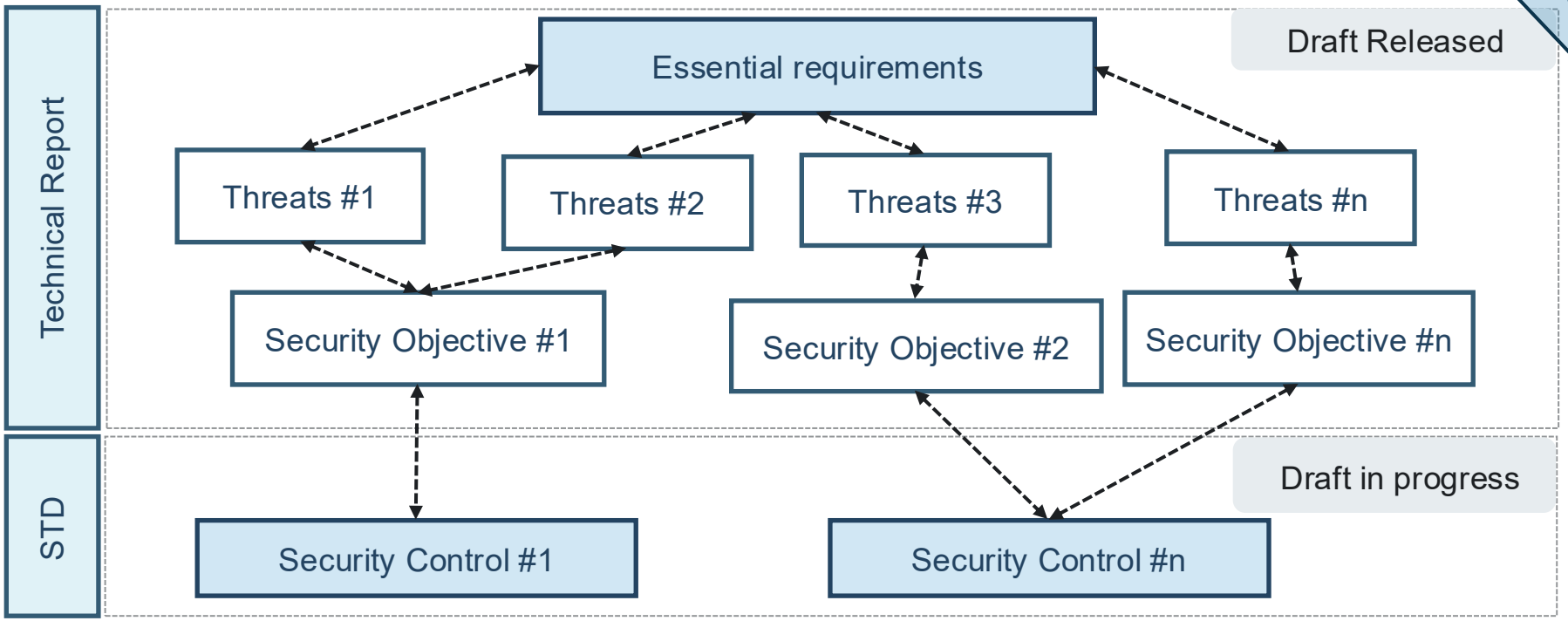
- Standardization request M/606 Annex I part II, the 2-14th (see also CEN, CENELEC and ETSI Work Programme) to be published by **30/10/2027**.
- Shall support the development of further, granular vertical harmonised standards for specific products or product types
- Shall support manufacturers in defining and implementing the security requirements for their products that fall into the default category
- In general, will be a catalogue of security controls with their objectives and more technical assessment criteria
- Builds upon the EN 18031:2024 series, augmented with additional security controls to cover the scope of CRA
- Provides a mapping of the essential requirements to these security controls
- It will include at least provisions related to the
  - Security problem definition
  - Security objectives
  - Technical specification of security requirements,
  - Assessment methodology.

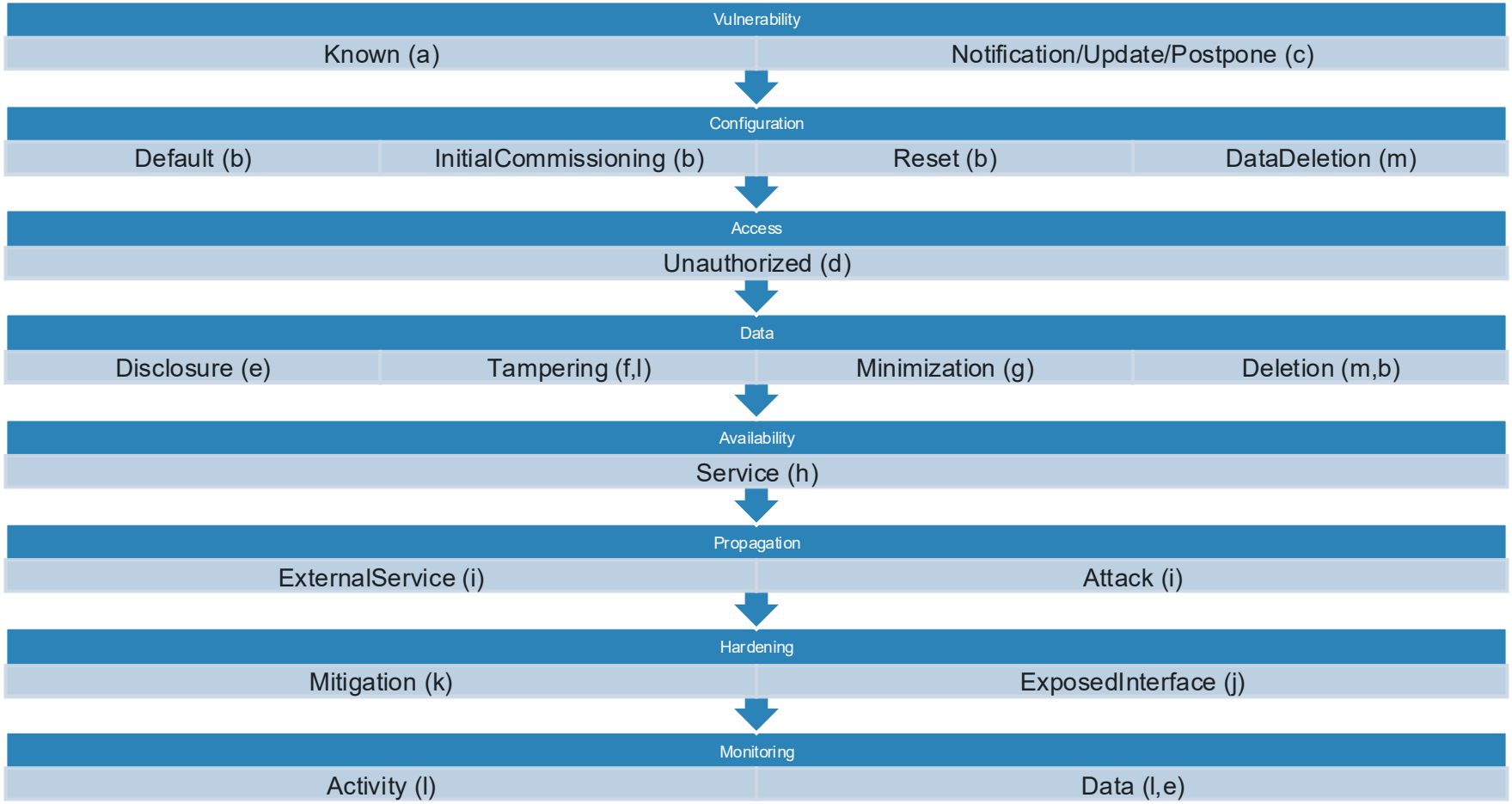
High level expected timeline



Note: This is indicative and will be adapted as we will process higher priority items

PT2 Artifacts – Technical Report




Vulnerability
Known (a)
Notification/Update/Postpone (c)
Configuration
Default (b)
InitialCommissioning (b)
Reset (b)
DataDeletion (m)
Access
Unauthorized (d)
Data
Disclosure (e)
Tampering (f,l)
Minimization (g)
Deletion (m,b)
Availability
Service (h)
Propagation
ExternalService (i)
Attack (i)
Hardening
Mitigation (k)
ExposedInterface (j)
Monitoring
Activity (l)
Data (l,e)

CEN/CLC/JTC 13

Date: 2024-03-04

prEN XXX

Secretariat: DIN

WI Number: JT013091

Cybersecurity requirements for products with digital elements – Generic Security Requirements

ICS:

PT2 structure

General (how to apply the standard)

- Risk based approach, method to demonstrate compliance ➔ Aligned to PT1
- System level considerations
- Dependence on manufacturer and user processes

Essential Requirements [Annex I.2.(a) – Annex I.2.(m)]

- Mapping to security objectives (refers/aligns to but is not limited to the TR)
- No applicability statements desired, handled by the Regulatory Risk Assessment
- No specific assessment criteria

Security objectives (a.k.a. Security Capabilities or Security Mechanisms)

- Informative mapping to control requirements
- Applicability will be determined later whether this is needed
- No assessment criteria

Control requirements Requirements

- Applicability to be determined
- Assessment criteria

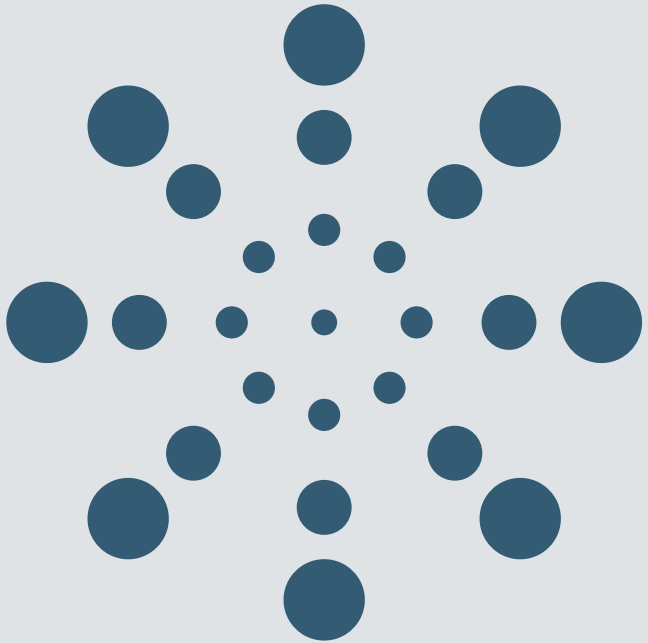
Informative annex(es)

- Mapping of the essential requirements or Security objectives to other standards (62443-4-2, 27002, 303645, etc. if you want to include something you have to provide the mapping)

04

Essential Requirements Deep Dive

Understanding of the essential requirements and relevant implications



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

Term and definition

- (41) **'exploitable vulnerability'** means a vulnerability that has the potential to be effectively used by an adversary under **practical operational conditions**;
- (40) **'vulnerability'** means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat;

Recitals (CRA)

- (54) … For that purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential cybersecurity requirements in order to make available their products with digital elements **without known exploitable vulnerabilities that might have an impact on the security of those products** and to appropriately apply suitable harmonised standards, common specifications or European or international standards.
- (66) … The **European vulnerability database** will assist manufacturers in **detecting known exploitable vulnerabilities** in their products, in order to ensure that secure products are made available on the market.

Article 13 – Obligations of manufacturers

- 1. **When placing a product with digital elements on the market**, manufacturers shall ensure that it has been designed, developed, and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

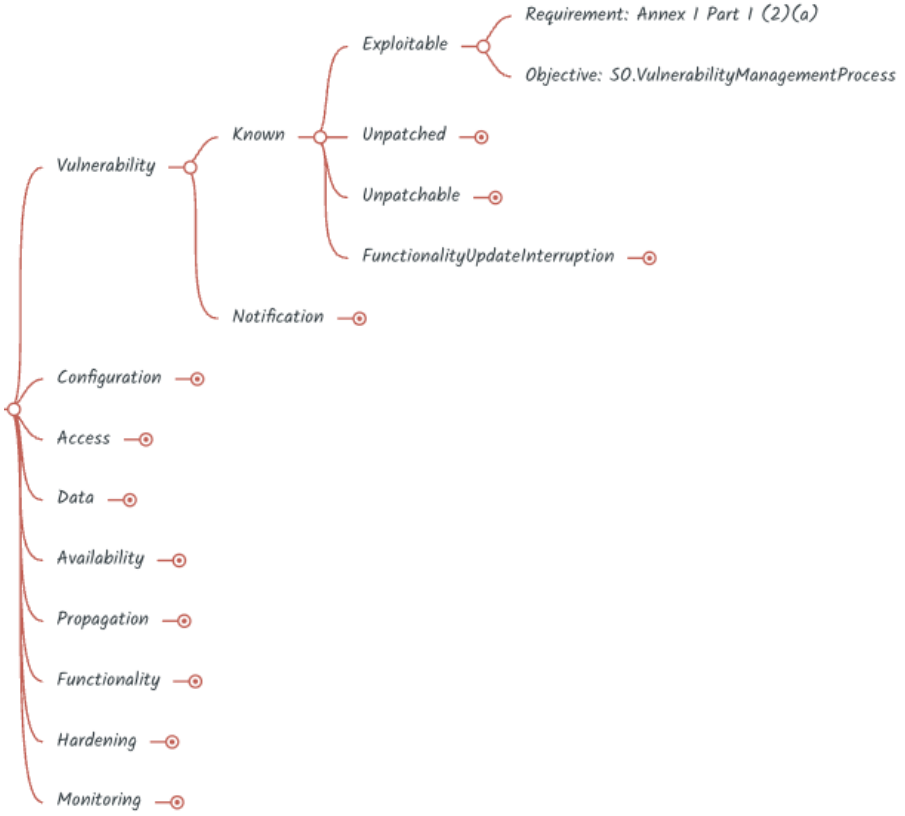
Questions from FAQs on the CRA implementation (PDF):

- **4.2.2 How can a manufacturer ensure that a product is free from all vulnerabilities?**
  - Not required to be free of all vulnerability – not all the vulnerabilities are exploitable under practical operational conditions
- **4.2.3 How should manufacturers deal with known exploitable vulnerabilities discovered after a product has been placed on the market but before reaching its final user?**
  - The obligation to deliver, on the basis of the risk assessment, products without known exploitable vulnerabilities applies at the moment of placement on the market (Article 13(1)).
- **5.1 How can a manufacturer become aware of an actively exploited vulnerability or a severe incident?**
  - The manufacturer may be required to provide a security update for the device, as soon as it is put into operation by its user.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ (d) are provided, on a risk basis, with up-to-date software and hardware at the moment of **placing on the market** that do not contain publicly **known exploitable vulnerabilities** as regards harm to the network or its functioning or misuse of network resources;

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (c) are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly **known exploitable vulnerabilities** as regards data protection and privacy;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ (c) are provided, on a risk basis, with up-to-date software and hardware at the moment of **placing on the market** that do not contain publicly **known exploitable vulnerabilities** as regards financial or monetary data;

Spoiler Alert – We have EN 18031-1:2024, EN 18031-2:2024, and EN 18031-3:2024 - Let's continue to build on them!

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

Threat	Security Objective
Threat.KnownVulnerabilityExploitation	SO.VulnerabilityManagementProcess

Mapping with 18031-X:2024
[GEC] General equipment capabilities • [GEC-1] Up-to-date software and hardware ~~with no publicly~~ without known exploitable vulnerabilities

Added security controls
NO ADDITION

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

Quick review of the verticals standards:

- Different approach and mentioning:
  - Vulnerability scanning, explicitly, automatically, and freely available scanners
  - Some mention EUVD,
  - Mostly refer to prEN 40000-1-3

How is 62443-4-2 approaching it?

- Ref. EN IEC 62443-4-1:2018/prAA (Process requirement)

Questions:

- What is the impact of mandating prEN 40000-1-3
  - In the vertical standards?
  - In the horizontal standards?

Personal reflections:

- **Verticals:**
  - Could make sense to refer normatively to prEN 40000-1-3 if provide presumptions of conformity – the preference is to have it informative
- **Horizontal:**
  - I believe that prEN 40000-1-3 should be informative only / But clear that there is a strong relationship

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

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

Think tank exercise on what could be required

The manufacturers should understand how they can become aware of a vulnerability and have the right process in place to check when it is exploitable based on practical conditions

- **Different way possible**
  - An external researcher who is reporting a vulnerability, accompanied by the relative exploitation
  - Internal security assessments/monitoring
  - A communication from a partners/supplier
- **What can you do as a minimum**
  - Maintain a list of assets and vulnerabilities
  - Check against the EUVD and verify that a specific vulnerability is not exploitable under operating conditions
    - prEN 4000-1-3 (SBOM /Ongoing monitoring / Triaging)
  - The selection of hardware and software component they play a role in the final product, so due diligence in the supply chain is desired

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (a) - Vulnerability Assessment

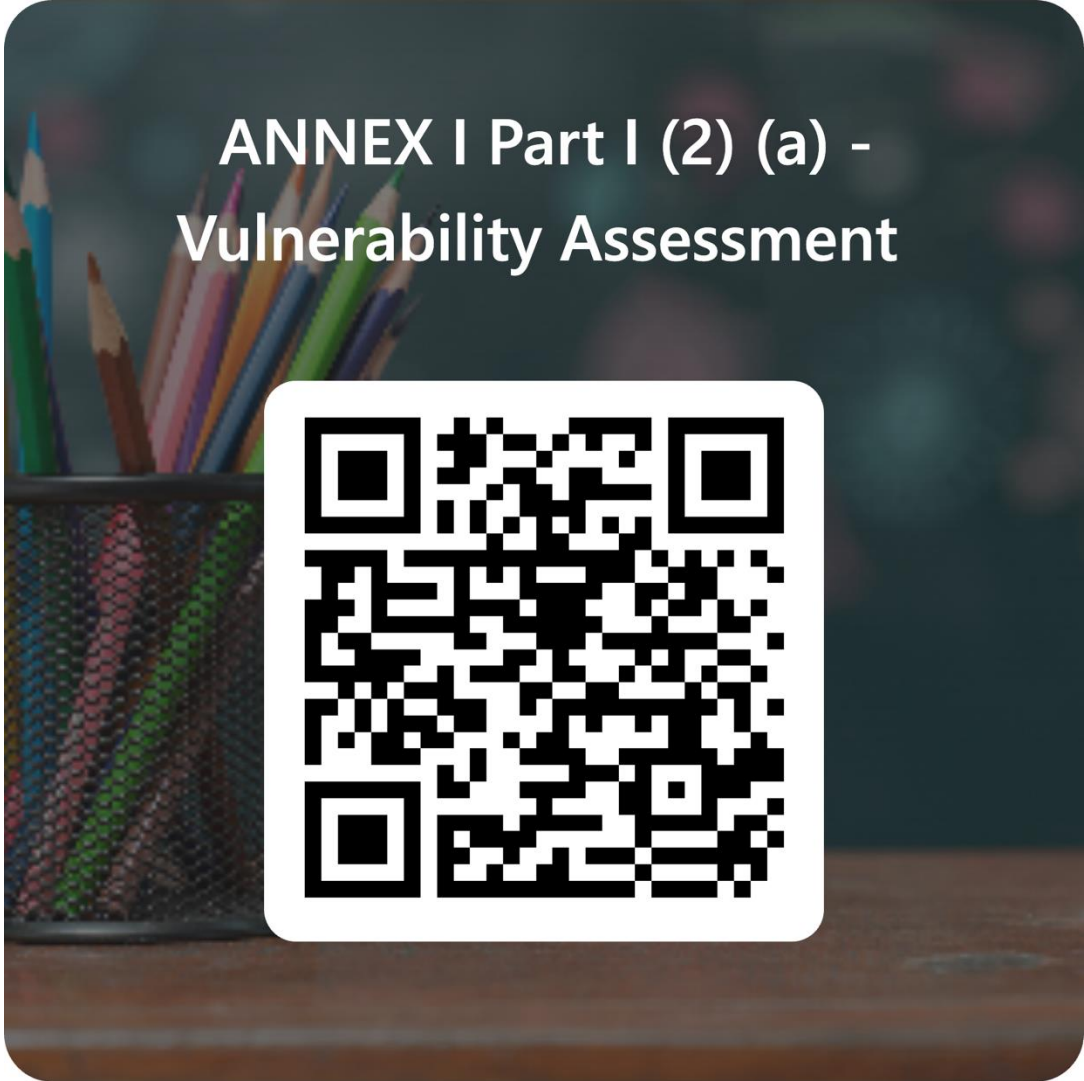
- (a) be made available on the market without known exploitable vulnerabilities;

Security Objective	Technical controls
SO.VulnerabilityManagementProcess	**[GEC] General equipment capabilities (EN 18031)** • [GEC-1] Up-to-date software and hardware with no ~~publicly~~ known exploitable vulnerabilities (EN 18031)

CONCLUSION – Essential requirement (a) fairly covered as in this mapping

Survey (a)

- You are invited to answer this section of the survey
- Survey [LINK]



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Term and definition

- N/A

Recitals (CRA)

- (64) Manufacturers should make their products with digital elements available on the market with a **secure by default configuration** and provide security updates to users free of charge. Manufacturers should be able to deviate from the essential cybersecurity requirements only for tailor-made products fitted to a particular purpose for a particular business user, where both the manufacturer and the user have explicitly agreed to a different set of contractual terms.

Article 13 – Obligations of manufacturers

- 1. **When placing a product with digital elements on the market**, manufacturers shall ensure that it has been designed, developed, and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

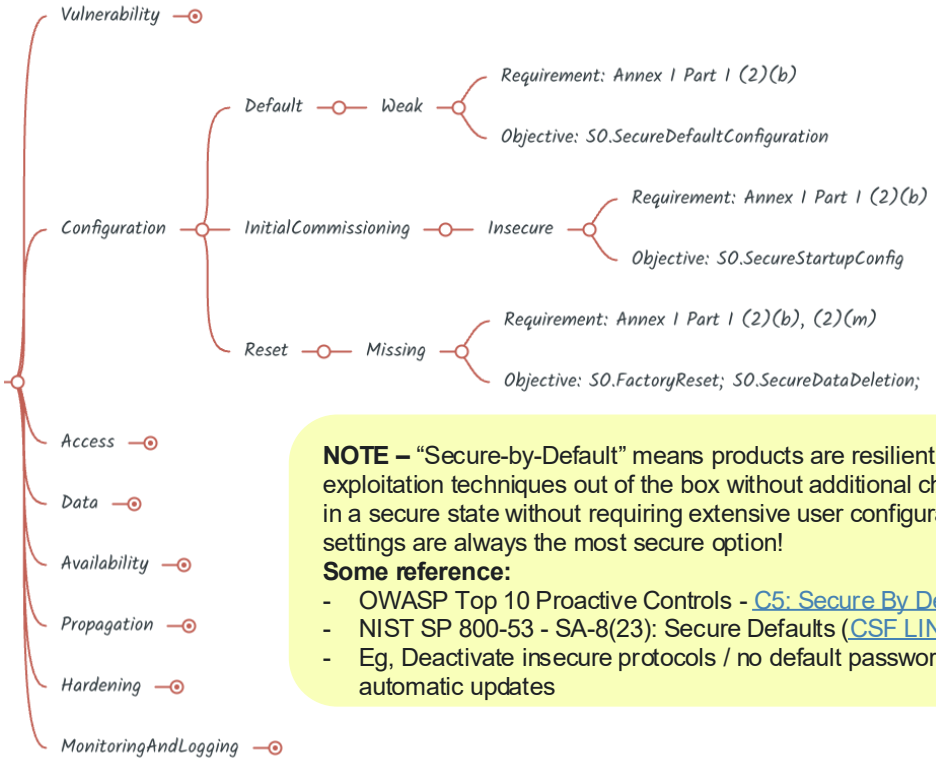
Questions from FAQs on the CRA implementation (PDF):

- **4.2.4 How does the secure-by-default requirement work?**
  - *Manufacturers are required to place products with digital elements on the market with a secure by default configuration, in light of that product's intended purpose and reasonably foreseeable use, and on the basis of the manufacturer's cybersecurity risk assessment.*
- ***4.2.5 When is a product "tailor-made"?* What documentation is required in these cases?**
  - *This could be the case, for example, for custom-developed hardware or software designed to meet the needs of a specific business user, or products that are developed for integration into a specific customer's highly controlled environments (e.g. closed networks or air-gapped environments) and are subject to specific contractual terms.*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;



NOTE – "Secure-by-Default" means products are resilient against prevalent exploitation techniques out of the box without additional charge. Software should start in a secure state without requiring extensive user configuration, ensuring the default settings are always the most secure option!

Some reference:

- OWASP Top 10 Proactive Controls - C5: Secure By Default Configurations
- NIST SP 800-53 - SA-8(23): Secure Defaults (CSF LINK)
- Eg, Deactivate insecure protocols / no default passwords / least privilege / automatic updates

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (g) allow users to easily delete their stored personal data**, enabling the disposal or replacement** of equipment without the risk of exposing personal data;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ -

NOTE – we have identified requirements from EN 18031-1:2024, EN 18031-2:2024, and EN 18031-3:2024, which can support the objectives of this essential requirement!

- Limit the exposure of services
- Documentation on exposed interfaces
- No unnecessary interface
- Documentation on sensing capability
- No default password
- Deletion mechanism

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Threat	Security Objective
Threat.UnsecureDefaultConfigExploitation	SO.SecureDefaultConfiguration
Threat.StartupConfigExploitation	SO.SecureStartupConfig
Threat.MissingResetFunctionalityConfigExploitation	SO.FactoryReset
Threat.MissingResetFunctionalityMalwareExploitation	
Threat.MissingResetFunctionalityDataExtraction	

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Mapping with 18031-X:2024

[GEC] General Equipment Capabilities
- [GEC-2] Limit exposure of services via related network interfaces
- [GEC-3] Configuration of optional services and the related exposed network interfaces
- [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces
- [GEC-5] No unnecessary external interfaces
- [GEC-7] Documentation of external sensing capabilities

[AUM] Authentication mechanism
- [AUM-5] Password strength
  - [AUM-5-1] Requirement for factory default passwords
  - [AUM-5-2] Requirement for non-factory default passwords

[DLM] Deletion Mechanisms
- [DLM-1] Applicability of deletion mechanisms

Added security controls

[GEC] General Equipment Capabilities
- [GEC-9] Secure startup configuration
- [GEC-10] Factory Reset
- [GEC-12] No Unneeded Software Components

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Quick review of the vertical standards:

- By nature, they have to be and are specific to their product category

How is 62443-4-2 approaching it?

- *CR 1.5 – Authenticator management (CR 1.5 RE (1))*
- *CR 3.14 – Integrity of the boot process (CR 3.14 RE (1))*
- *CR 4.2 – Information persistence (CR 4.2 RE (1), CR 4.2 RE (2))*
- *CR 7.4 – Control system recovery and reconstitution*
- *CR 7.6 – Network and security configuration settings (CR 7.6 RE (1))*
- *CR 7.7 – Least functionality*

Some reflections

- It would be desirable to have alignment with the naming of the catalogue of controls and minimal shared control for each category – based also on the current prEN 40000-1-4 (PT2)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Recap: Quick scan and extract from verticals

- ❑ Unwanted exposed interface software and hardware
- ❑ The configuration data are not appropriately secured
- ❑ Improper permissions and lack of segregation
- ❑ Default or weak credentials
- ❑ Unsecure protocols
- ❑ Unsecure crypto and hashing functions
- ❑ *Unsecure startup configuration - first-time configuration*
- ❑ Identification of tampering of critical configuration data
- ❑ Missing or weak reset functionality
- ❑ Missing or insecure deletion mechanisms (part of essential requirement - m)
- ❑ Outdated and vulnerable firmware or software (part of essential requirement - a)
- ❑ Data minimization

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (b) - Secure Configuration

(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 product with digital elements, including the possibility to reset the product to its original state;

Security Objective	Technical Controls
SO.SecureDefaultConfiguration	**[GEC] General equipment capabilities (EN 18031)** • [GEC-2] Limit exposure of services via related network interfaces (EN 18031) • [GEC-3] Configuration of optional services and the related exposed network interfaces (EN 18031) • [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces (EN 18031) • [GEC-5] No unnecessary external interfaces (EN 18031) • [GEC-7] Documentation of external sensing capabilities (EN 18031) • [GEC-12] No Unneeded Software Components (NEW) **[AUM] Authentication mechanism** • [AUM-5] Password strength (EN 18031) • [AUM-5-1] Requirement for factory default passwords (EN 18031)
SO.SecureStartupConfig	**[GEC] General equipment capabilities (EN 18031)** • [GEC-9] Secure startup configuration (NEW) **[AUM] Authentication mechanism** • [AUM-5] Password strength (EN 18031) • [AUM-5-2] Requirement for non-factory default passwords(EN 18031)
SO.FactoryReset	**[DLM] Deletion Mechanisms** • [DLM-1] Secure Data deletion mechanisms (Applicability of deletion mechanisms) (EN 18031) **[GEC] General equipment capabilities** • [GEC-10] Factory Reset (NEW)

Survey (b)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Term and definition

- N/A

Recitals

- (1) Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and **the insufficient and inconsistent provision of security updates** to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.
- (31) in relation to **Directive (EU) 2024/2853 (Product Liability Directive)**

  It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault (strict liability). Where such a lack of safety consists **in a lack of security updates** after the placing on the market of the product, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates should be laid down in this Regulation.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Recitals (CRA)

- **(56)** Manufacturers should therefore design their products and put in place processes to ensure that products with digital elements include functions that enable the notification, distribution, download and installation of security updates automatically, in particular in the case of consumer products. They should also provide the possibility to approve the download and installation of the security updates as a final step. Users should retain the ability to deactivate automatic updates, with a clear and easy-to-use mechanism, supported by clear instructions on how users **can opt out**. …
  - Irrespective of whether a product with digital elements is designed to receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay.
  - **Where a product with digital elements has a user interface or similar technical means allowing direct interaction with its users, the manufacturer should make use of such features to inform users that their product with digital elements has reached the end of the support period.** Notifications should be limited to what is necessary in order to ensure the effective reception of this information and should not have a negative impact on the user experience of the product with digital elements.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Questions from FAQs on the CRA implementation (PDF):

- **4.3.3 Is the manufacturer responsible for the installation of security updates by the product's users?**
  - … The manufacturer is not responsible under the CRA if the user does not install security updates, e.g. where updates are not installed either because automatic updates are not applicable or because the user opts out. ….
- ***2.3.1 What is the interplay between the CRA and the Product Liability Directive?***
  - … For example, the CRA provides for specific obligations for manufacturers regarding security updates for products with digital elements (Annex I). …

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

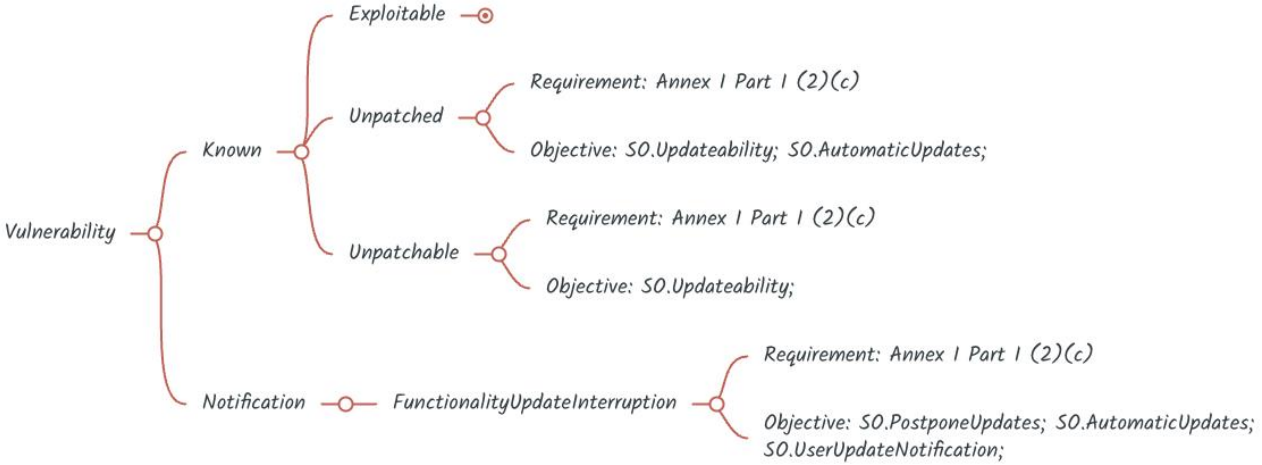
Recitals (CRA)

- (56) …Manufacturers should therefore design their products and put in place processes to ensure that products with digital elements include functions that **enable the notification, distribution, download and installation of security updates automatically, in particular in the case of consumer products**. They should also provide the possibility to **approve the download and installation of the security updates as a final step**. Users should retain the ability to deactivate automatic updates, with a clear and **easy-to-use** mechanism, supported by clear instructions on **how users can opt out. ….**

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ (e) are provided with **automated** and **secure mechanisms for updating software or firmware** that allow, when necessary, the mitigation of vulnerabilities that if exploited **may lead to the radio equipment harming the network or its functioning or the misuse of network resources**;

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (d) are provided with **automated** and **secure mechanisms for updating software or firmware** that allow, when necessary, the mitigation of vulnerabilities that if exploited **may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of personal data**;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ (d) are provided with **automated** and **secure mechanisms for updating software or firmware** that allow, when necessary, the mitigation of vulnerabilities that if exploited **may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of financial or monetary data**;

NOTE – Some additional consideration:

- Appropriate timeframe enabled as default setting
- Clear and easy to use opt mechanisms
- Temporary postponing update
- Notification of available updates

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Threat	Security Objective
Threat.UnpatchableVulnerabilityExploitation	SO.Updateability
Threat.UnpatchedVulnerabilityExploitation	SO.AutomaticUpdates
Threat.MissingUpdateNotificationExploitation	SO.UserUpdateNotification
Threat.FunctionalityUpdateInterruption	SO.PostponeUpdates

NOTE – The major concerns are related to:

- The challenge is about Remote Data Processing – it's possible that manufacturers use a silent-patching approach on the "cloud component" side.
- How to deal with an appropriate timeline and timely updates / how much the product can facilitate this aspect
- Opt-out mechanisms we are still evaluating how to be integrated

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Mapping with 18031-X:2024

[SUM] Secure update mechanism
- [SUM-1] Applicability of update mechanisms
- [SUM-2] Secure updates
- [SUM-3] Automated updates

Added security controls

[SUM] Secure update mechanism
- [SUM-4] Postponed Updates

[UNM] User notification mechanism
- [UNM-4] User Security Update Notifications (NEW) (Possibility that will be merged in SUM-4)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Think tank exercise on what could be required

- ❑ Updatability
- ❑ Secure updates
- ❑ Automatic updates where appropriate
- ❑ User notification of available update with the option to postpone the installation
- ❑ Opt-out Mechanisms for update

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (c) - Security Updates

(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;

- **Some extracted requirements from verticals**
  - Some specific requirements such as update signature verification, timing jitter, and transparency logging
  - Secure update
  - Some mention anti-rollback
  - Documentation on secure updates
- **How is 62443-4-2 approaching it?**
  - CR 3.10 – Support for updates
    - CR 3.10 RE (1) – Update authenticity and integrity
    - CR 3.10 RE (2) – Automatic updates
- **Initiatives in progress:**
  - Cross-vertical initiative on Secure Update to find alignment

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

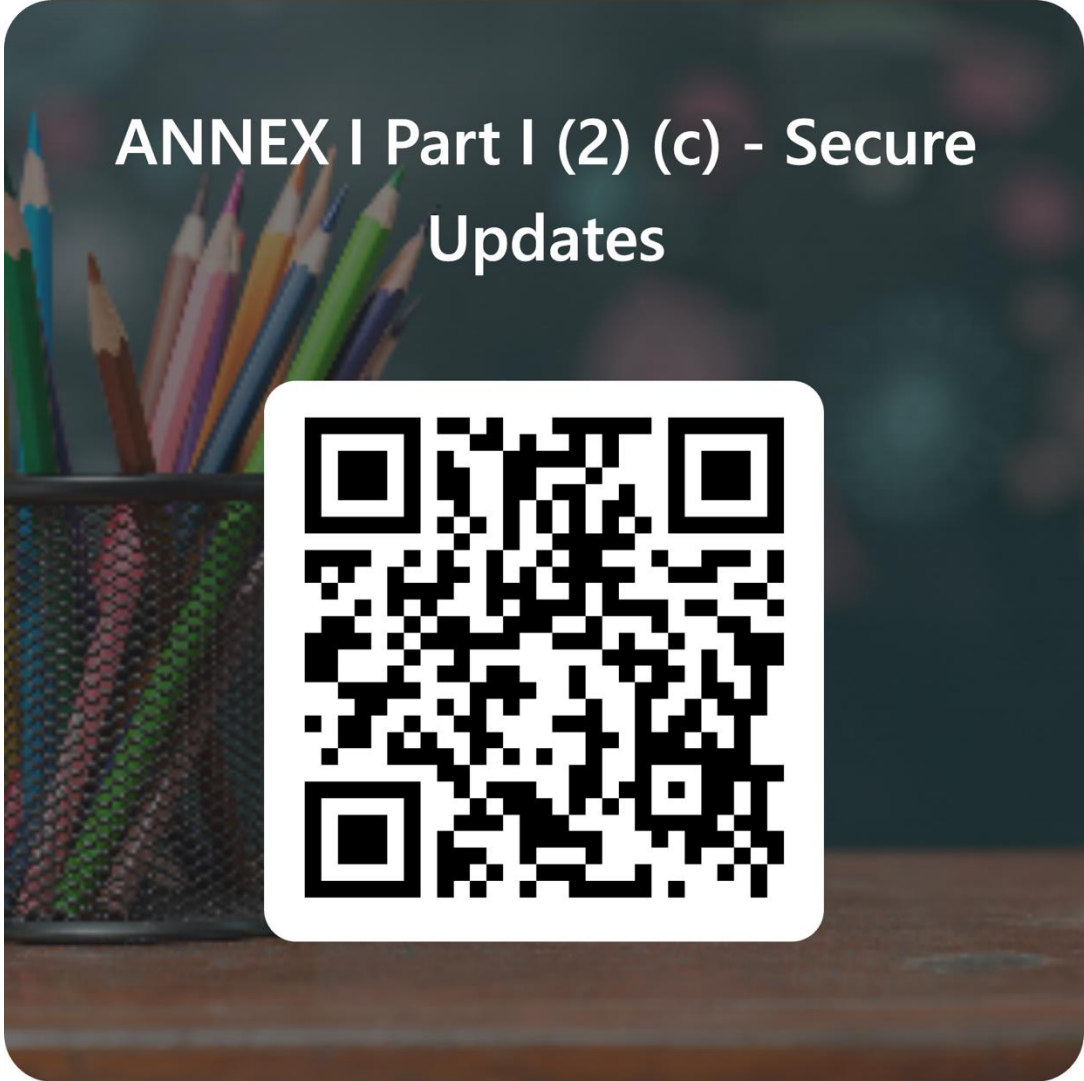
ECR ANNEX I Part I (2) (c) - Security Updates

(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;

Security Objective	Technical Controls
SO.Updateability	**[SUM] Secure update mechanism** • [SUM-1] Applicability of update mechanisms (EN 18031) • [SUM-2] Secure updates (EN 18031)
SO.AutomaticUpdates	**[SUM] Secure update mechanism** • [SUM-3] Automated updates (EN 18031)
SO.UserUpdateNotification	**[UNM] User notification mechanism** • [UNM-4] User Security Update Notifications (NEW) • (Possibility that will be merged in SUM-4)
SO.PostponeUpdates	**[SUM] Secure update mechanism** • [SUM-4] Postponed Updates (NEW)

Survey (c)

- You are invited to answer this section of the survey
- Survey [LINK]



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

Term and definition

- In EN 62443-4-2, the reporting is at the moment equivalent to the notification
- event notification: act of reporting the occurrence of an event to 'interested' objects (from: ISO/IEC 23004-7:2008(en), 3.1.41)
- Alert: An alert is a message that is sent to a system or a person as a notification of a significant event that may require immediate attention. (LINK)

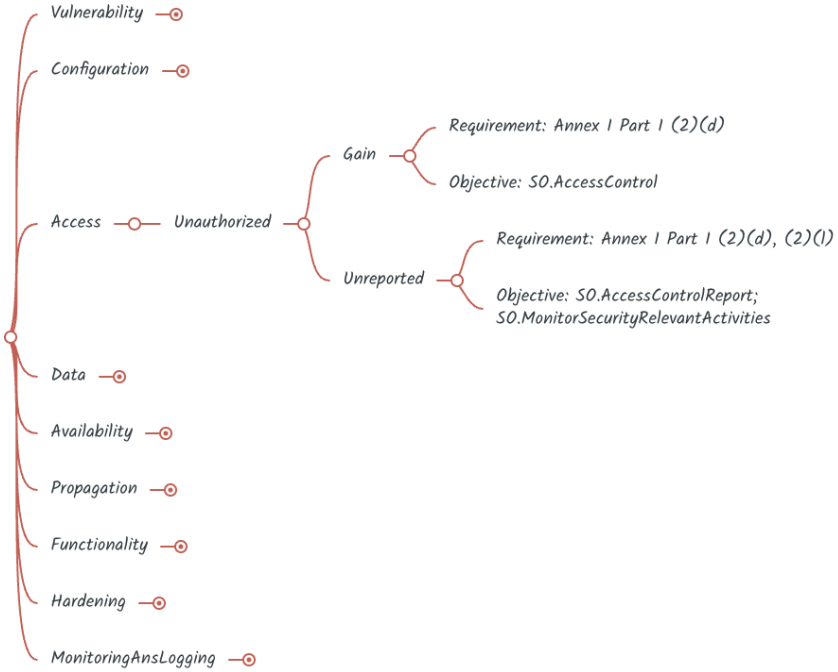
Recitals

- N/A

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ (c) implement appropriate **authentication and access control mechanisms;**

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (b) implement appropriate **authentication and access control mechanisms;**

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ (b) implement appropriate **authentication and access control mechanisms;**

NOTE – The list of relative controls in EN 18031-X:2024 meets the CRA requirements.

- It is already clear that a major gap needs to be filled from this view – a report **on possible unauthorised access.**

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

Threat	Security Objective
Threat.UnauthorizedAccess	SO.AccessControl
Threat.NotReportedUnauthorizedAccess	SO.AccessControlReport

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

Mapping with 18031-X:2024

[ACM] Access control mechanism

- [ACM-1] Applicability of access control mechanisms (VOID)
- [ACM-2] Appropriate access control mechanisms (MERGE ACM-1 ACM2)

Mapping with 18031-X:2024

[AUM] Authentication mechanism

- [AUM-1] Applicability of authentication mechanisms (VOID)
  - [AUM-1-1] Requirement network interface (VOID)
  - [AUM-1-2] Requirement user interface (VOID)
  - [AUM-1-3] Requirement machine interface (VOID)
- [AUM-2] Appropriate authentication mechanisms (MERGE AUM-1 AUM-2)
- [AUM-3] Authenticator validation
- [AUM-4] Changing authenticators
- [AUM-5] Password strength
  - [AUM-5-1] Requirement for factory default passwords
  - [AUM-5-2] Requirement for non-factory default passwords
- [AUM-6] Brute force protection

Added security controls

[GEC] General Equipment Capabilities

- [GEC-13] Report on possible unauthorised access and corruption (NEW)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

How is 62443-4-2 approaching it?

- *CR 1.1 – Human user identification and authentication (CR 1.1 RE (1), CR 1.1 RE (2)*
- *CR 1.2 – CR 1.14*
- *CR 2.1 – Authorization enforcement (CR 2.1 RE (1), CR 2.1 RE (2), CR 2.1 RE (3), CR 2.1 RE (4))*
- *CR 2.2 – Wireless use control*
- *CR 2.5 – Session lock*
- *CR 2.6 – Remote session termination*
- *CR 2.8 – Auditable events*
- *CR 2.13 – Use of physical diagnostic and test interfaces*
- *CR 3.11 – Physical tamper resistance and detection*
  - *CR 3.11 RE (1) – Notification of a tampering attempt*
- *CR 3.13 – Provisioning asset owner roots of trust*
- *CR 4.3 – Use of cryptography*
- *CR 6.1 – Audit log accessibility*
- *CR 6.2 – Continuous monitoring*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (d) - Access Control

(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;

Security Objective	Technical Controls

SO.AccessControl	**[ACM] Access control mechanism**
	• [ACM-1] Applicability of access control mechanisms (EN 18031) (VOID)
	• [ACM-2] Appropriate access control mechanisms (EN 18031) (MERGE ACM-1 ACM2)
	[AUM] Authentication mechanism
	• [AUM-1] Applicability of authentication mechanisms (EN 18031) (VOID)
	  • [AUM-1-1] Requirement network interface (EN 18031) (VOID)
	  • [AUM-1-2] Requirement user interface (EN 18031) (VOID)
	  • [AUM-1-3] Requirement machine interface (EN 18031) (VOID)
	• [AUM-2] Appropriate authentication mechanisms (EN 18031) (MERGE AUM-1 AUM-2)
	  • [AUM-2-1] Requirement one-factor authentication (EN 18031)
	  • [AUM-2-2] Requirement multi-factor authentication (EN 18031)
	• [AUM-3] Authenticator validation (EN 18031)
	• [AUM-4] Changing authenticators (EN 18031)
	• [AUM-5] Password strength (EN 18031)
	  • [AUM-5-1] Requirement for factory default passwords (EN 18031)
	  • [AUM-5-2] Requirement for non-factory default passwords (EN 18031)
	• [AUM-6] Brute force protection (EN 18031)

SO.AccessControlReport	**[GEC] General Equipment Capabilities** • [GEC-13] Report on possible unauthorised access and corruption (NEW)

Survey (d)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

Term and definition

- **Confidentiality** means keeping data secret from everyone except those we want to have access to it. The ISO/IEC 27000:2018 defines it as "*The property that information is not made available or disclosed to unauthorized individuals, entities, or processes*."

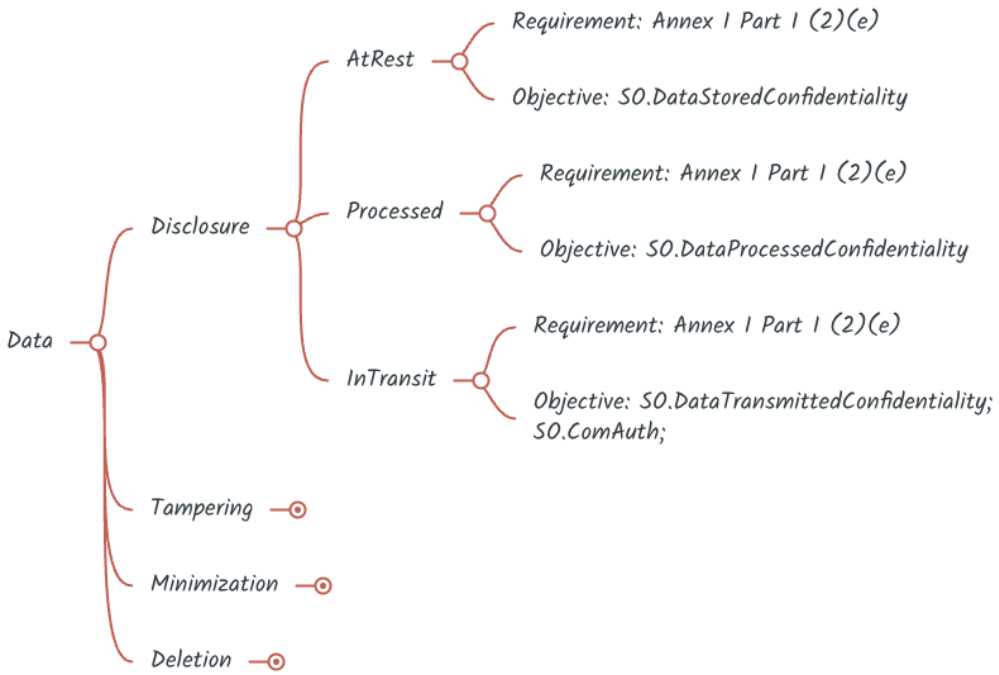
Recitals

- N/A

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- (a) **protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage**, access, **disclosure,** destruction, loss or alteration or lack of availability;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- (a) **protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorised processing, including storage**, access, **disclosure**, destruction, loss or alteration or lack of availability;

NOTE – The list of relative controls in EN 18031-X:2024 meets the CRA requirements. It is already clear that there is less emphasis on the **state of the art mechanisms**.

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

Threat	Security Objective
Threat.DataAtRestDisclosure	SO.DataStoredConfidentiality
Threat.DataProcessedDataDisclosure	SO.DataProcessedConfidentiality
Threat.DataInTransitDisclosure	SO.DataTransmittedConfidentiality
	SO.ComAuth

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

Mapping with 18031-X:2024
[SSM] Secure storage mechanism • [SSM-1] Applicability of secure storage mechanisms • [SSM-3] Appropriate confidentiality protection for secure storage mechanisms **[SCM] Secure communication mechanism** • [SCM-3] Secure communication mechanisms with confidentiality protection • [SCM-4] Appropriate replay protection for secure communication mechanisms **[CCK] Confidential cryptographic keys** • [CCK-1] Appropriate CCKs • [CCK-2] CCK generation mechanisms • [CCK-3] Preventing static default values for preinstalled CCKs **[CRY] Cryptography** • [CRY-1] Best practice cryptography

Added security controls
NO ADDITION

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

Think tank exercise on what could be required

- Encrypt data, personal data in transit and at rest
- Keep cryptography up to date and in line with the best practices
- Ensure proper access controls
- Let's keep in mind that confidentiality cannot be reached only by encryption, but also:
  - Isolation
  - Seclusion / Data compartmentalization
  - Access control
  - Least privilege
  - Network security controls
  - Zero trust
  - Secure storage
  - Etc.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

The approach followed by verticals

- Great work is underway in EUSR across the Crypt cross-verticals group – the objective is to create a reusable Annex K for all the vertical and to be integrated also in the horizontal standard.
  - ***K.1 State of the Art Cryptography (SOTA)***
    - Annex K defines an "allow list" approach to cryptographic mechanisms in CRA, based on the from "ECCG Agreed Cryptographic Mechanisms" (ACM):
      - https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
  - ***K.2. Requirement ("crypto agility")***

Some reflections / Notes

- There are concerns and discussions that are happening with manufacturers that are worried about products with legacy cryptography algorithms, against a fixed list of approved algorithms
- Concerns about the evaluation process when an algorithm is not listed in the approved list
  - Eg, What would we do in case we have a modern algorithm such as ChaCha20 Poly1305 – not also present in https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

How is 62443-4-2 approaching it?

- *CR 1.2 – Software process and device identification and authentication*
- *CR 1.14 – Strength of symmetric key-based authentication*
- *CR 2.13 – Use of physical diagnostic and test interfaces*
- *CR 3.11 – Physical tamper resistance and detection*
- *CR 3.13 – Provisioning asset owner roots of trust*
- *CR 4.1 – Information confidentiality (CR 4.1 RE (1))*
- *CR 4.2 – Information persistence*
  - *CR 4.2 RE (1) – Erase of shared memory resources*
  - *CR 4.2 RE (2) – Erase verification*
- ***CR 4.3 – Use of cryptography***

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (e) - Confidentiality (Disclosure)

(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;

Security Objective	Technical Controls
SO.DataStoredConfidentiality	**[SSM] Secure storage mechanism** • [SSM-1] Applicability of secure storage mechanisms • [SSM-3] Appropriate confidentiality protection for secure storage mechanisms
SO.DataProcessedConfidentiality	**[GEC] General Equipment Capabilities** • [GEC-8] Product Integrity
SO.DataTransmittedConfidentiality	**[SCM] Secure communication mechanism** • [SCM-3] Secure communication mechanisms with confidentiality protection • [SCM-4] Appropriate replay protection for secure communication mechanisms
SO.ComAuth	**[SCM] Secure communication mechanism** • [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms • [SSM-3] Appropriate confidentiality protection for secure storage mechanisms
SO.SecureProvisioning	**[CCK] Confidential cryptographic keys** • [CCK-1] Appropriate CCKs • [CCK-2] CCK generation mechanisms • [CCK-3] Preventing static default values for preinstalled CCKs **[CRY] Cryptography** • [CRY-1] Best practice cryptography

Survey (e)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

Term and definition

- **Integrity** means detecting whether data has been corrupted or manipulated, intentionally or unintentionally, by entities. The ISO/IEC 27000:2018 defines it as "*The property of accuracy and completeness*."

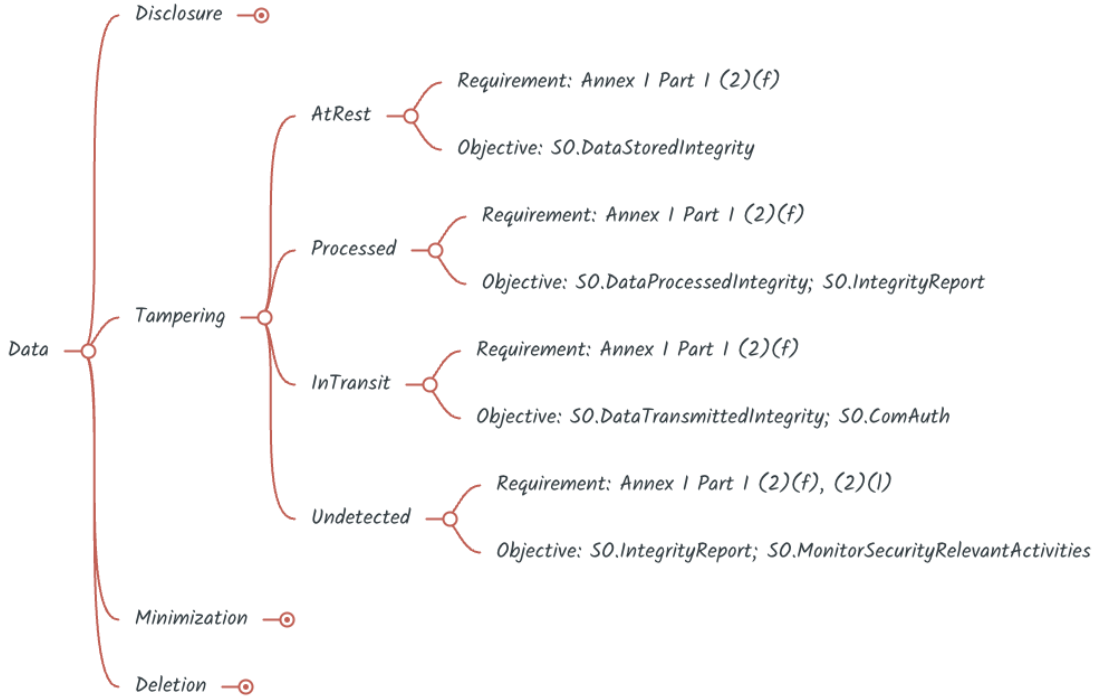
Recitals

- N/A

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- (a) **protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage**, access, disclosure, destruction, loss or **alteration** or lack of availability;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- (a) **protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorised processing, including storage**, access, **disclosure**, destruction, loss or **alteration** or lack of availability;

NOTE – the main observations are the following:
- It is already clear that the focus is on personal data and should be extended to include commands and programs.
- The other gap is about the **report on corruption** as per the (d) authorized access case.

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

Threat	Security Objective
Threat.DataAtRestTampering	SO.DataStoredIntegrity
Threat.DataInTransitTampering	SO.DataTransmittedIntegrity
	SO.ComAuth
Threat.ProcessedDataTampering	SO.DataProcessedIntegrity
Threat.TamperingUndetected	SO.IntegrityReport

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

Mapping with 18031-X:2024

[SSM] Secure storage mechanism
- [SSM-1] Applicability of secure storage mechanisms
- [SSM-2] Appropriate integrity protection for secure storage mechanisms

[SCM] Secure communication mechanism
- [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

[GEC] General Equipment Capabilities
- [GEC-8] Product Integrity

Added security controls

[GEC] General Equipment Capabilities
- [GEC-13] Report on possible unauthorised access and corruption (NEW)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

Think tank exercise on what could be required

- ❑ Establish state-of-the-art mechanisms to guarantee integrity
- ❑ Verification is possible to check for corruption or manipulation
- ❑ Secure boot is a way to provide a mechanism to ensure integrity on the boot sequence and processes
- ❑ If integrity fails, the device should be able to restore integrity
- ❑ Notification system to communicate that a tampering/corruption happened

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

How is 62443-4-2 approaching it?

- ❑ *CR 1.8 – Public key infrastructure certificates*
- ❑ *CR 1.9 – Strength of certificate-based authentication*
- ❑ *CR 1.14 – Strength of symmetric key-based authentication*
- ❑ *CR 2.8 – Auditable events*
- ❑ *CR 2.11 – Timestamps*
- ❑ *CR 2.13 – Use of physical diagnostic and test interfaces*
- ❑ *CR 3.1 – Communication integrity*
- ❑ *CR 3.4 – Software and information integrity*
  - ❑ *CR 3.4 RE (1) – Authenticity of software and information*
  - ❑ *CR 3.4 RE (2) – Automated notification of integrity violations*
- ❑ *CR 3.8 – Session integrity*
- ❑ *CR 3.10 RE (1) – Update authenticity and integrity*
- ❑ *CR 3.11 – Physical tamper resistance and detection*
  - ❑ *CR 3.11 RE (1) – Notification of a tampering attempt*
- ❑ *CR 3.14 – Integrity of the boot process*
- ❑ ***CR 4.3 – Use of cryptography***
- ❑ *CR 7.3 RE (1) – Backup integrity verification*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (f) - Integrity (Tampering)

(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;

Security Objective	Technical Controls
SO.DataStoredIntegrity	**[SSM] Secure storage mechanism** • [SSM-1] Applicability of secure storage mechanisms • [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms
SO.DataProcessedIntegrity	**[GEC] General Equipment Capabilities** • [GEC-8] Product Integrity
SO.DataTransmittedIntegrity	**[SCM] Secure communication mechanism** • [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms
SO.ComAuth	**[SCM] Secure communication mechanism** • [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms (EN 18031) • [SSM-3] Appropriate confidentiality protection for secure storage mechanisms
SO.IntegrityReport	**[GEC] General Equipment Capabilities** • [GEC-13] Report on possible unauthorised access and corruption (NEW)

Survey (f)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

Term and definition

- The data minimisation principle is expressed in **Article 5(1)(c) of the GDPR and Article 4(1)(c)** of **Regulation (EU) 2018/1725**, which provide that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Recitals

- N/A

References:

- ISO/IEC 27701:2025 - Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance
- ISO/IEC 29100:2024 - Information technology — Security techniques — Privacy framework (FREE ACCESS - LINK)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

Questions from FAQs on the CRA implementation (PDF):

- **2.8.1 What is the interplay between the CRA and the General Data Protection Regulation?**
  - The CRA and the General Data Protection Regulation (GDPR) are of a different nature and there is no legal overlap… the GDPR provides for requirements for personal data processing activities, **such as data minimisation** and data integrity and confidentiality principles (Article 5 GDPR), the obligation for data protection by design (Article 25 GDPR), data security (Article 32 GDPR), and the notification of personal data breaches (Article 33 GDPR), which may contribute to the cybersecurity of products with digital elements. However, the manufacturer's compliance for a product with digital elements with the requirements of the CRA does not have any formal impact on the tools used by controllers or processors under the GDPR to demonstrate compliance of the processing of personal data with the GDPR (such as by means of codes of conduct (Article 40 GDPR) or certification schemes (Article 42 GDPR)).

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- (e) include functionalities to inform the user of changes that may affect data protection and privacy;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- -

NOTE – Here, there is a gap to fill with new requirements
- The notification part of EN 18031 will be reused, but doesn't cover the objectives from this essential requirement

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

Threat	Security Objective
Threat.UnnecessaryDataMisuse	SO.DataMinimization

Mapping with 18031-X:2024

[UNM] User notification mechanism
- [UNM-1] Applicability of user notification mechanisms
- [UNM-2] Appropriate user notification content

Added security controls

[DTM] Data minimization
- [DTM-1] Data minimisation in relation to intended purpose
- [DTM-2] Default Data Processing Minimisation
- [DTM-3] Configurable Controls for Optional Data Processing

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

Think tank exercise on what could be required

- Process requirements
  - DATA CLASSIFICATION, LABELLING, AND WHATEVER IS LINKED WITH THE DATA LIFECYCLE
- Technical controls that can be linked to this essential requirement:
  - Minimize the storing and processing of data that is sufficient and necessary for its function and intended purpose
  - Data shall be disposed of when no longer needed for a legitimate purpose
  - Mechanism that allows the user to:
    - to control permission to elaborate on specific information
    - define the useful lifetime of the data (for how long the information can be used)
    - to provide functionality for opt-in and opt-out
    - To notify a change in privacy and processing of information due to an update or changes
  - Effective data anonymization/tokenization
  - Differential privacy
  - The product shall offer a mechanism to monitor if there is data

EXAMPLE – You could also monitor your IoT products and services for any security anomalies or flaws – for example, telemetry information that can allow you to identify unusual circumstances early and deal with them. This minimises security risk and allows you to resolve problems quickly.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

The approach followed by verticals (quick scan)

- Storage isolation, timing analysis, user consent, privacy by design, no collection of PII without explicit consent, minimize disclosure of information, encrypt all sensitive data, employ encrypted channels, explicit consent for collecting additional telemetry data collection beyond the intended purpose shall require

How 62443-4-2 is approaching it?

- *CR 2.1 – Authorization enforcement,*
  - *CR 2.1 RE (1) – Authorization enforcement for all users (humans, software processes and devices)*
  - *CR 2.1 RE (2) – Permission mapping to roles*
  - *CR 2.1 RE (3) – Supervisor override*
  - *CR 2.1 RE (4) – Dual approval*

Some reflections

- Data minimisation is a new topic for the IoT world
- There is a lot of fragmentation, and it is natural because we are defining now the technical principles related not only to process but to product capability
- Let's find together a common baseline

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (g) - Data Minimization

(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 product with digital elements (data minimisation);

Security Objective	Technical Controls
SO.DataMinimization	**[UNM] User notification mechanism (EN 18031)** • [UNM-1] Applicability of user notification mechanisms (EN 18031) • [UNM-2] Appropriate user notification content (EN 18031) **[DTM] Data minimization (NEW)** • [DTM-1] Data minimisation in relation to intended purpose (NEW) • [DTM-2] Default Data Processing Minimisation (NEW) • [DTM-3] Configurable Controls for Optional Data Processing (NEW)

Survey (g)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

Term and definition

- **'incident'** means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;
  - '**incident**' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;
- '**incident having an impact on the security of the product with digital elements**' means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions;

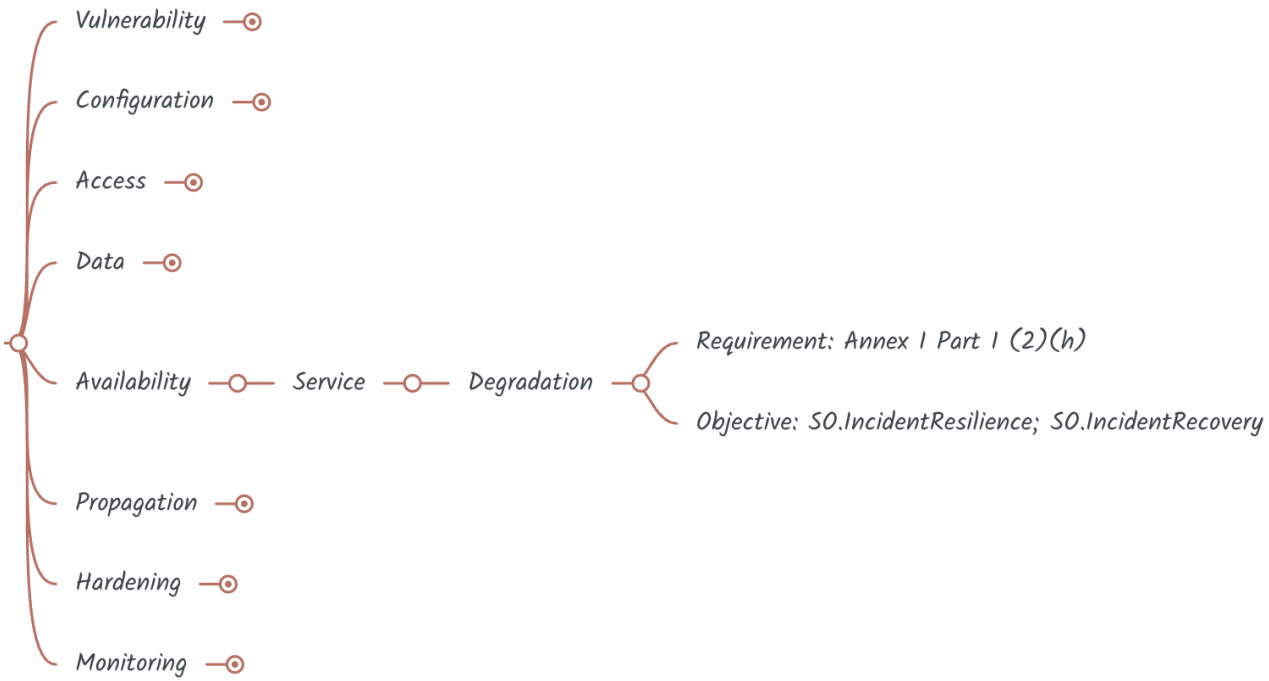
Recitals

- **ANNEX II INFORMATION AND INSTRUCTIONS TO THE USER**
  - At minimum, the product with digital elements shall be accompanied by:
  - ….
    - 4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the **product's essential functionalities** and information about the security properties;

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ **(b) are designed to mitigate the effects of ongoing denial of service attacks;**
- ❑ (d) are provided, on a risk basis, **with up-to-date software** and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards **harm to the network or its functioning** or misuse of network resources;

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (a) protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or **lack of availability**;
- ❑ (d) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or **lack of availability of personal data;**

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ (a) protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration **or lack of availability;**
- ❑ (d) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or **lack of availability of financial or monetary data;**

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

Threat	Security Objective
Threat.AvailabilityDegradationAfterIncident	SO.IncidentRecovery
Threat.AvailabilityDegradationDuringIncident	SO.IncidentResilience

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

Mapping with 18031-X:2024
[RLM] Resilience mechanism • [RLM-1] Applicability and appropriateness of resilience mechanisms

Added security controls
[RLM] Resilience mechanism • [RLM-2] Recovery from incidents • [RLM-3] Network prioritization (NEW) • [RLM-4] Resource prioritization (NEW) • [RLM-5] Resource management (NEW) • [RLM-6] Control system backup (NEW)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

Think tank exercise on what could be required

- ❑ Fail-safe- Enable graceful recovery after interruption (eg, power loss, network disconnection, software crashes) – return to an operational state and verify integrity
  - ❑ Self-diagnose and check for log inconsistency
- ❑ Support core functionality without remote dependencies where appropriate
- ❑ Resistance to denial of service attacks or any other targeted attack, such as resource exhaustion, including rate limiting and connection throttling.
- ❑ Redundancy where applicable
- ❑ Segregation/isolation of important functions/fault isolation
- ❑ Least privilege

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

How is 62443-4-2 approaching it?

- CR 2.7 – Concurrent session control
- CR 2.9 – Audit storage capacity
- CR 2.10 – Response to audit processing failures
- CR 3.5 – Input validation
- CR 3.9 RE (1) – Audit records on write-once media
- CR 1.9 RE (1) – Hardware security for public key-based authentication
- CR 7.2 – Resource management
- *CR 7.3 – Control system backup*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (h) - Availability

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

Security Objective	Technical Controls
SO.IncidentRecovery	**[RLM] Resilience mechanism** • [RLM-2] Recovery from incidents (NEW)
SO.IncidentResilience	**[RLM] Resilience mechanism** • [RLM-1] Applicability and appropriateness of resilience mechanisms (EN 18031) • [RLM-3] Network prioritization (NEW) • [RLM-4] Resource prioritization (NEW) • [RLM-5] Resource management (NEW) • [RLM-6] Control system backup (NEW)

Survey (h)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

Term and definition

- (37)'**cybersecurity risk**' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;
- (38)'**significant cybersecurity risk**' means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe **negative impact**, including by causing considerable material or non-material loss or disruption;

Recitals

- (43) Products with digital elements should be considered to be important **if the negative impact of the exploitation of potential vulnerabilities in the product can be severe due to, inter alia, the cybersecurity-related functionality or a function carrying a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.**
- (44) … An incident involving important products with digital elements that fall under class II might lead to **greater negative impacts** than an incident involving important products with digital elements that fall under class I ….

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- (a) include elements to monitor and control network traffic, including the transmission of outgoing data;
- (d) are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that **do not contain publicly known exploitable vulnerabilities as regards harm to the network or its functioning or misuse of network resources**;
- (e) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, **the mitigation of vulnerabilities that if exploited may lead to the radio equipment harming the network or its functioning or the misuse of network resources;**

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- -

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- -

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

Threat	Security Objective
Threat.ExtServiceAvailabilityDegradation	SO.LimitExternalImpact
	SO.PreventAttackPropagation
	SO.MonitorExternalImpact

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

Mapping with 18031-X:2024

[GEC] General equipment capabilities
- [GEC-8] Product Integrity

[TCM] Traffic Control Mechanism
- [TCM-1] Applicability of and appropriate traffic control mechanisms (EN 18031)

[NMM] Network monitoring mechanism
- [NMM-1] Applicability and appropriateness of network monitoring mechanisms

Added security controls

[LIM] External impact limitation
- [LIM-1] External impact limitation
- [LIM-2] Prevention of attack propagation

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

Think tank exercise on what could be required

- Manage the resources
  - Network (eg. Rate limiting / throttling / Load Balancing / retry/Backoff)
  - Computational (eg. CPU)
  - Storage (eg. Monitoring the exhaustion of space – “static and dynamic quotas”)
- Error handling and documentation of external interface
- Robust API and communication design
- Use of well-defined protocols with management of recovery and error states
- Isolation and segmentation when applicable
- Least privilege for services
- Input validation

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

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

How is 62443-4-2 approaching it?

- ❑ CR 1.13 – Access via untrusted networks
- ❑ CR 2.8 – Auditable events
- ❑ CR 3.5 – Input validation
- ❑ CR 3.6 – Deterministic output
- ❑ *CR 5.1 – Network segmentation*
- ❑ *CR 5.2 – Zone boundary protection*
- ❑ *CR 7.1 – Denial of service protection*

Source: *C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (i) – Minimize negative impact

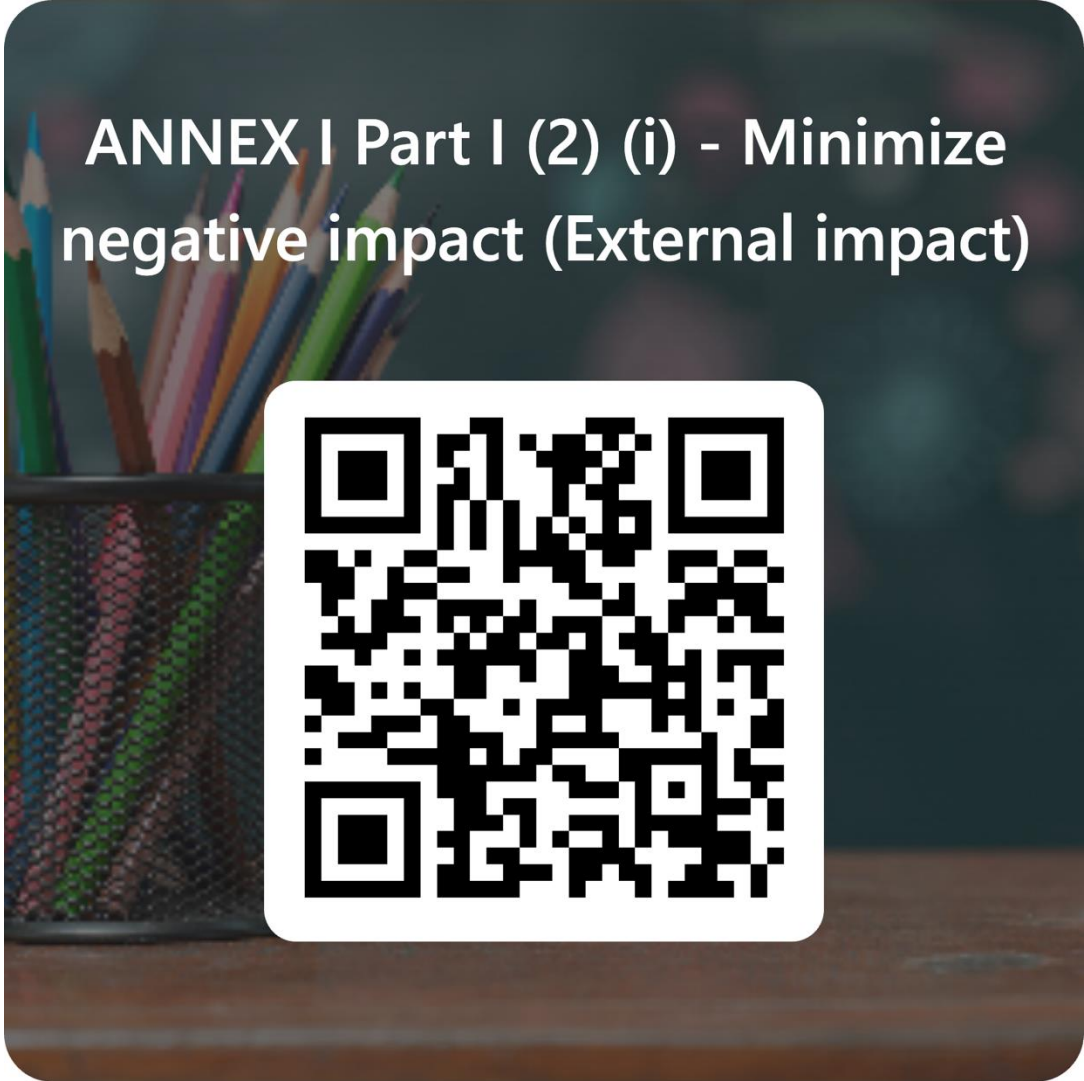
(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

Security Objective	Technical Controls
SO.LimitExternalImpact	**[GEC] General equipment capabilities (EN 18031)** • [GEC-8] Product Integrity (EN 18031) **[TCM] Traffic Control Mechanism (EN 18031)** • [TCM-1] Applicability of and appropriate traffic control mechanisms (EN 18031) **[LIM] External impact limitation (NEW)** • [LIM-1] External impact limitation (NEW)
SO.PreventAttackPropagation	**[TCM] Traffic Control Mechanism (EN 18031)** • [TCM-1] Applicability of and appropriate traffic control mechanisms (EN 18031) **[LIM] External impact limitation (NEW)** • [LIM-2] Prevention of attack propagation (NEW)
SO.MonitorExternalImpact	**[NMM] Network monitoring mechanism** • [NMM-1] Applicability and appropriateness of network monitoring mechanisms (EN 18031)

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

Survey (i)

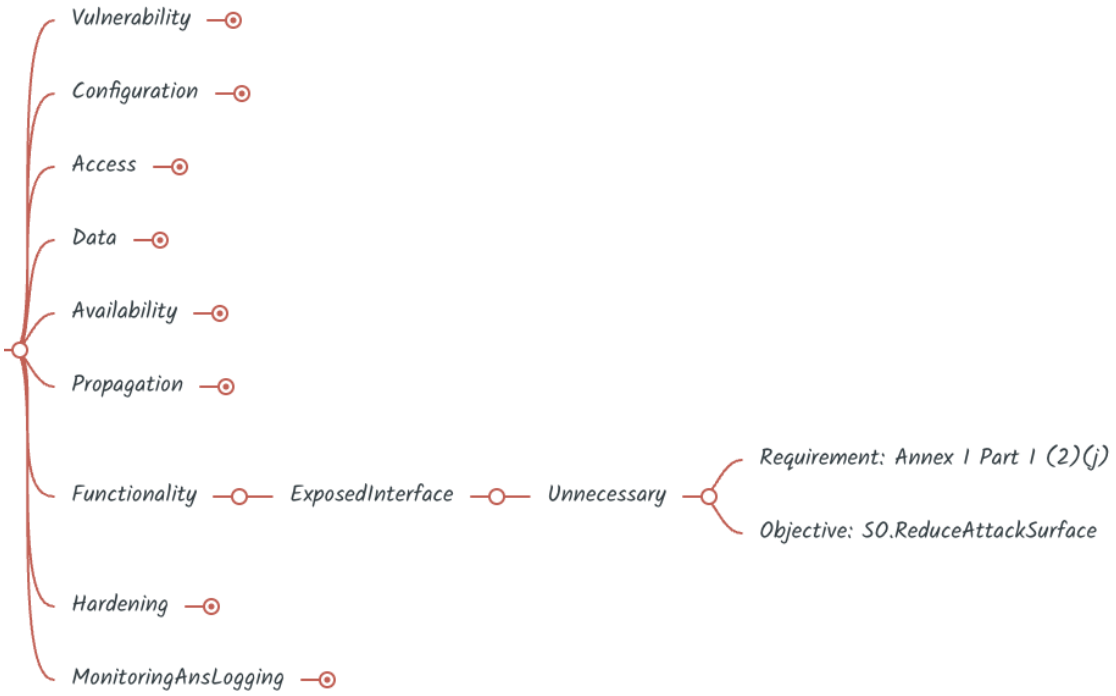
- You are invited to answer this section of the survey
- Survey [LINK]



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- (f) **protect the exposed attack surfaces and minimise the impact of successful attacks.**

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- (h) **protect the exposed attack surfaces and minimise the impact of successful attacks**.

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- (f) **protect the exposed attack surfaces and minimise the impact of successful attacks.**

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

Threat	Security Objective
Threat.UnnecessaryFunctionalityExploitation	SO.ReduceAttackSurface

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

Mapping with 18031-X:2024

[GEC] General equipment capabilities
- [GEC-2] Limit exposure of services via related network interfaces
- [GEC-3] Configuration of optional services and the related exposed network interfaces
- [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces
- [GEC-5] No unnecessary external interfaces
- [GEC-6] Input validation
- [GEC-7] Documentation of external sensing capabilities

Added security controls

[GEC] General equipment capabilities
- [GEC-12] No Unneeded Software Components

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

Think tank exercise on what could be required

- ❑ Identify and document the presence of all the interfaces, hardware and software (ag. API)
- ❑ Disable what is not essential (“secure by default”)
- ❑ Use secure protocols and components where possible.
- ❑ Conduct periodic attack surface review
- ❑ Access control, Least privilege, and zoning/compartmentalization can be important
- ❑ Input validation
- ❑ Remove or disable unused services, ports, protocols
- ❑ Minimize connectivity when it is not required
- ❑ Provide the user option to enable and disable services and protocols based on what he is using

Useful references:
- OWASP - Attack Surface Analysis Cheat Sheet (LINK)
- ETSI EN 303 645 V3.1.3 - 5.6 Minimize exposed attack surfaces (LINK)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

How is 62443-4-2 approaching it?

- CR 1.13 – Access via untrusted networks
- CR 2.4 – Mobile code
- CR 2.5 – Session lock
- CR 2.8 – Auditable events
- CR 3.5 – Input validation
- CR 5.1 – Network segmentation
- CR 5.2 – Zone boundary protection
- CR 7.7 – Least functionality

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (j) - Attack Surface Minimization

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

Security Objective	Technical Controls
SO.ReduceAttackSurface	**[GEC] General equipment capabilities** • [GEC-2] Limit exposure of services via related network interfaces (EN 18031) • [GEC-3] Configuration of optional services and the related exposed network interfaces (EN 18031) • [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces (EN 18031) • [GEC-5] No unnecessary external interfaces (EN 18031) • [GEC-6] Input validation (EN 18031) • [GEC-7] Documentation of external sensing capabilities (EN 18031) • [GEC-12] No Unneeded Software Components (NEW)

Survey (j)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

Term and definition

- **'incident'** means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;
  - '**incident**' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;
- '**incident having an impact on the security of the product with digital elements**' means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions;

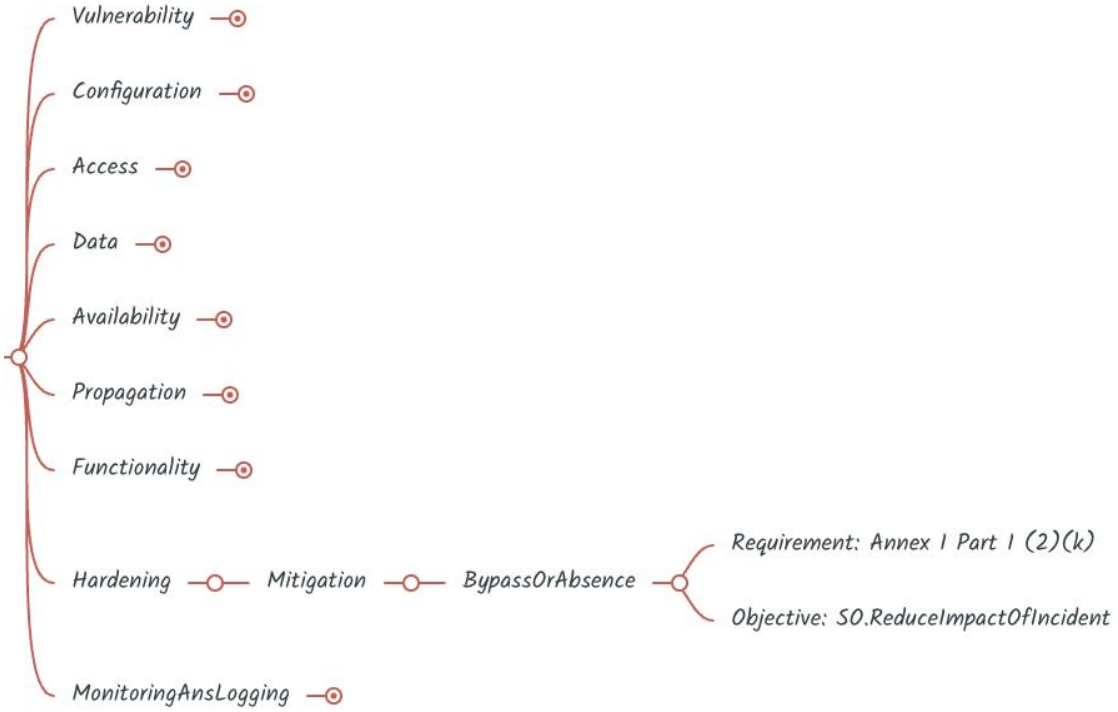
Recitals / Articles

- **Article 14 Reporting Obligations of manufacturers**
  - 5. For the purposes of paragraph 3, an **incident** having an impact on the security of the product with digital elements shall be considered to be **severe** where:
    - (a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or
    - (b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- -

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- -

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

Threat	Security Objective
Threat.ExploitationMitigationFailure	SO.ReduceImpactOfIncident

NOTE:
- Reduce the impact of eg. Priviledge escalation, lateral movement, malware installation, being part of a DDoS bootnet, injection exploits
- Attack path classification and models can be used Common Attack Pattern Enumeration and Classification (LINK)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

Mapping with 18031-X:2024
NO MAPPING

Added security controls
[GEC] General equipment capabilities • [GEC-11] Exploit mitigation mechanisms (NEW)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

Think tank exercise on what could be required

- Technical mitigation mechanisms (System / Software Level)
  - Address Space Layout Randomization (ASLR)
  - Data Execution Prevention (DEP)
  - Control-Flow Integrity (CFI)
  - Sandboxing
  - Signed Software Execution Policies
  - …..
- Design and development (Secure By Design)
  - Secure by default configuration
  - Memory safety managemenet
  - Vulnerability Assessment
  - …
- Operational & Strategic
  - Patch management
  - Application control / whitelisting\Network Segmentation
  - Disabling unnecessary services
  - Access Control
  - Least privilege
  - …

Useful references:

- ENISA - Guidelines for Securing the Internet of Things (Nov 2020, LINK)
- MITRE - CWE Top 25 Most Dangerous Software Weaknesses (Jan 2026, LINK)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

How is 62443-4-2 approaching it?

- CR 3.2 – Protection from malicious code
- CR 3.4 – Software and information integrity
- CR 3.6 – Deterministic output
- CR 3.7 – Error handling
- CR 7.1 – Denial of service protection
- CR 7.2 – Resource management
- CR 7.6 – Network and security configuration settings
- CR 7.7 – Least functionality
- *CR 7.9 – Component Reset*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

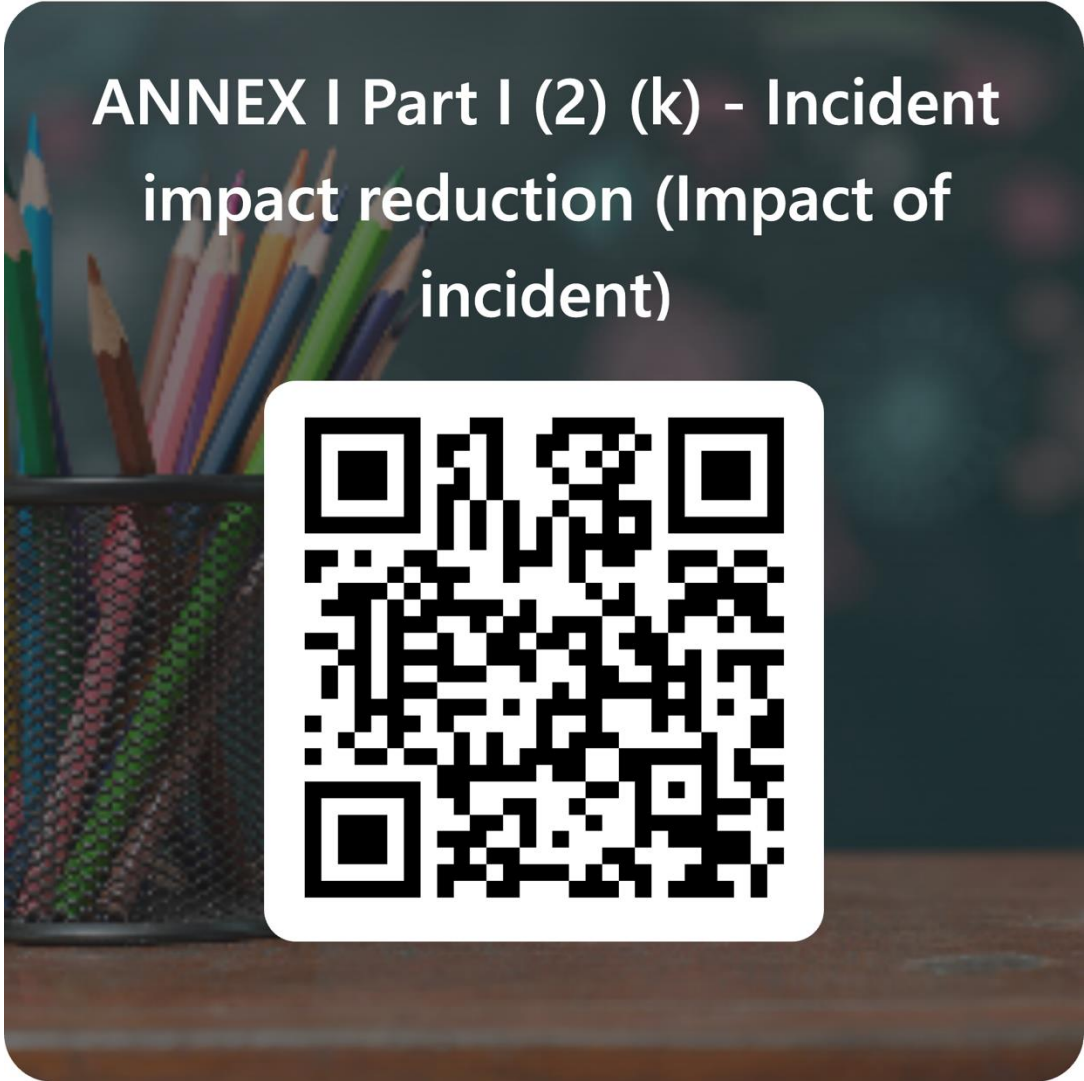
ECR ANNEX I Part I (2) (k) – Reduce Impact of Incident (Hardening/Exploit Mitigations)

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

Security Objective	Technical Controls
SO.ReduceImpactOfIncident	**[GEC] General equipment capabilities** • [GEC-11] Exploit mitigation mechanisms

Survey (k)

- You are invited to answer this section of the survey
- Survey [LINK]



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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**;

Term and definition

- **Logging:**
  - From ISO 27001:2022 - 8.15 – Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed
- **Monitoring activities**
  - From ISO 27001:2022 - 8.16 – Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
- **Alert:** An alert is a message that is sent to a system or a person as a notification of a significant event that may require immediate attention. (Ref: LINK)

Recitals

- N/A

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

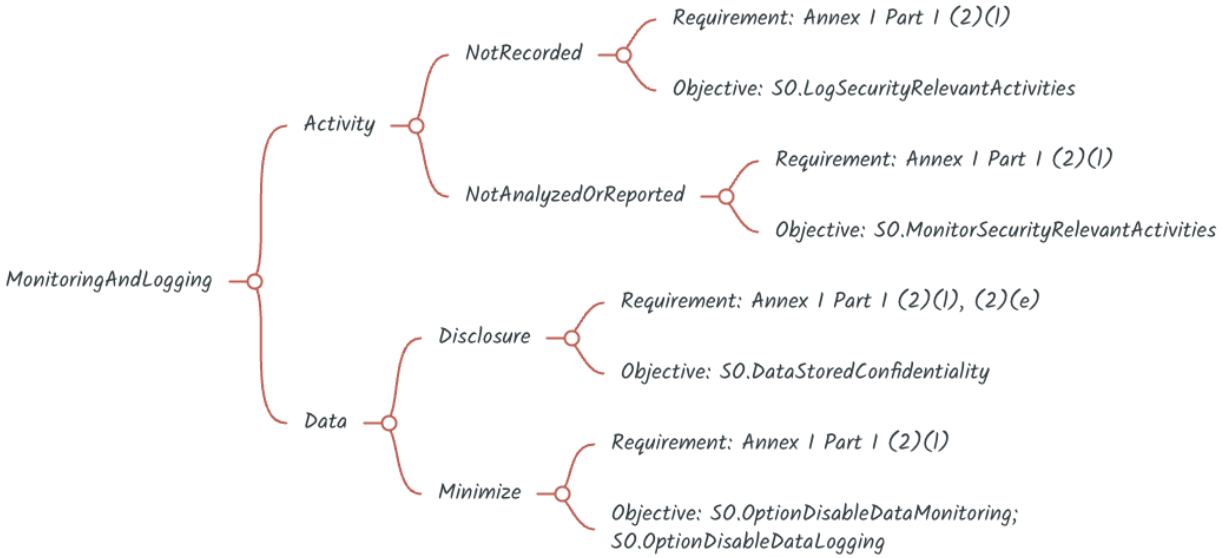
❑ NISTIR 8259A - IOT DEVICE CYBERSECURITY CAPABILITY CORE BASELINE (LINK)

Device Cybersecurity Capability	Common Elements	Rationale	IoT Reference Examples
Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.	1. The ability to report the device's cybersecurity state 2. The ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state 3. The ability to restrict access to the state indicator so only authorized entities can view it 4. The ability to prevent any entities (authorized or unauthorized) from editing the state except for those entities that are responsible for maintaining the device's state information 5. The ability to make the state information available to a service on another device, such as an event/state log server	• This capability supports vulnerability management and incident detection. • Cybersecurity state awareness helps enable investigating compromises, identifying misuse, and troubleshooting certain operational problems. • How the device makes other entities aware of a cybersecurity state will vary based on context-specific needs and goals, but may include capturing and logging information about events in a persistent record that may have to be stored off the device, sending signals to a monitoring system to be handled externally, or alerting via an interface on the IoT device itself.	• **CSDE**: 5.1.7 • **CTIA**: 4.7, 4.12, 5.7, 5.16 • **ENISA**: GP-TM-55, GP-TM-56 • **ETSI**: 4.7-2, 4.10-1 • **GSMA**: CLP13_6.13.1, 7.2.1, 9.1.1.2 • **IEC**: CR 2.8, CR 3.9, CR 6.1, CR 6.2 • **IIC**: 7.3, 7.5, 7.7, 8.9, 10.3, 10.4 • **IoTSF**: 2.4.7.5 • **NEMA**: Monitoring Devices and Systems • **OCF:** 5.1, 5.7, 8.6, 12, 13.8, 13.16 • **PSA**: C1.3, D1.1, D3.2, D3.4, D3.5, D5.1, R4.1, R4.3, R4.4

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- (a) include elements to **monitor** and control network traffic, including the transmission of outgoing data;

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- (f) **log the internal activity that can have an impact on data protection and privacy;**

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- (e) **log the internal activity that can have an impact on financial or monetary data;**

***Source**: C(2022)5637 – Standardisation request M/585 - https://ec.europa.eu/growth/tools-databases/enorm/mandate/585_en*

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

Threat	Security Objective
Threat.NotRecordedSecurityActivity	SO.LogSecurityRelevantActivities
Threat.NotMonitoredSecurityActivity	SO.MonitorSecurityRelevantActivities
Threat.UnnecessaryDataLogging	SO.OptionDisableDataLogging
Threat.UnnecessaryDataMonitoring	SO.OptionDisableDataMonitoring

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

Mapping with 18031-X:2024

[LGM] Logging mechanism
- [LGM-1] Applicability of logging mechanisms
- [LGM-2] Persistent storage of log data
- [LGM-3] Minimum number of persistently stored events
- [LGM-4] Time-related information of persistently stored dog data
- [LGM-6] Exclude sensitive personal information (NEW)

[NMM] Network monitoring mechanism
- [NMM-1] Applicability and appropriateness of network monitoring mechanisms

[TCM] Traffic control mechanism
- [TCM-1] Applicability of and appropriate traffic control mechanisms

Added security controls

[LGM] Logging mechanism
- [LGM-5] Disabling logging (NEW)

[MON] Monitoring of security Activities
- [MON-1] Monitor security relevant activities (NEW)
- [MON-2] Disable monitoring (NEW)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

Think tank exercise on what could be required

- ❑ Recording all the relevant changes and events
- ❑ Allow for detailed authentication and access log
- ❑ Monitor internal activities (service status, events, network behaviour)
- ❑ Important to store the logs securely (to allow integrity and authenticity)
- ❑ Minimize the type of information to the necessary one to not leak sensitive data
- ❑ Allow the user for having the possibility to opt out of the mechanism for logging/monitoring/notification where appropriate
- ❑ Logging and monitoring information shall be accessed only by authorized entities
- ❑ With monitoring, we can also add also notification mechanisms

Useful references:

- European Commission Information System Security Policy C(2006) 3602 - STANDARD ON LOGGING AND MONITORING (Brussels, 27/09/2010, LINK)
- CISA - Best Practices for Event Logging and Threat Detection (August 21, 2024, LINK)
- OWASP Cheat Sheet Series (LINK)
- ISO/IEC DIS 24970:2025-11 – Draft - Artificial intelligence - AI system logging (LINK)
- ETSI EN 303 645 V3.1.3 (2024-09) (LINK)
- NISTIR 8259A - IOT DEVICE CYBERSECURITY CAPABILITY CORE BASELINE (LINK)

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

How is 62443-4-2 approaching it?

- CR 1.12 – System use notification
- CR 2.8 – Auditable events
  - CR 2.8 RE (1) – Opt-out mechanism for authorized users
- CR 2.10 – Response to audit processing failures
- CR 2.11 – Timestamps
- CR 3.4 – Software and information integrity
  - CR 3.4 RE (1) – Authenticity of software and information
  - CR 3.4 RE (2) – Automated notification of integrity violations
- CR 6.1 – Audit log accessibility
  - CR 6.1 RE (1) – Programmatic access to audit logs
- CR 6.2 – Continuous monitoring

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (l) - Monitoring and Logging

(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;

Security Objective	Technical Controls
SO.LogSecurityRelevantActivities	**[LGM] Logging mechanism** • [LGM-1] Applicability of logging mechanisms (EN 18031) • [LGM-2] Persistent storage of log data (EN 18031) • [LGM-3] Minimum number of persistently stored events (EN 18031) • [LGM-4] Time-related information of persistently stored log data (EN 18031) • [LGM-6] Exclude sensitive personal information (NEW)
SO.MonitorSecurityRelevantActivities	**[NMM] Network monitoring mechanism** • [NMM-1] Applicability and appropriateness of network monitoring mechanisms (EN 18031) **[MON] Monitoring of security Activities** • [MON-1] Monitor security relevant activities (NEW)
SO.OptionDisableDataLogging	**[LGM] Logging mechanism** • [LGM-5] Disabling logging (NEW)
SO.OptionDisableDataMonitoring	**[MON] Monitoring of security Activities** • [MON-2] Disable monitoring (NEW)

Survey (I)

- You are invited to answer this section of the survey
- Survey [LINK]

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.**

Scope

- Deletion functionality is intended especially for situations involving a transfer of ownership, disposal, or third-party device maintenance.
- This functionality is also important when a device is used by multiple users (e.g., an infotainment system in a car rental situation). The ideal scenario is that the user should be able to delete all their data and configuration, leaving the system ready for the next user.
- Such a deletion functionality can potentially present an **attack vector.**

Term and definition

- From ETSI 303 645 - Deleting personal data "**easily**" means that minimal steps are required to complete that action that each involve minimal complexity.
- From 31700-1:2023 – **Deletion** is the: *process by which personally identifiable information (PII) (3.2) is changed in a manner so that it is no longer present, recognizable or usable and can only be reconstructed with excessive effort*
  - Note 1 to entry: The term "**deletion**" covers the following: disposition mechanism, erasure, destruction, destruction of data storage media.

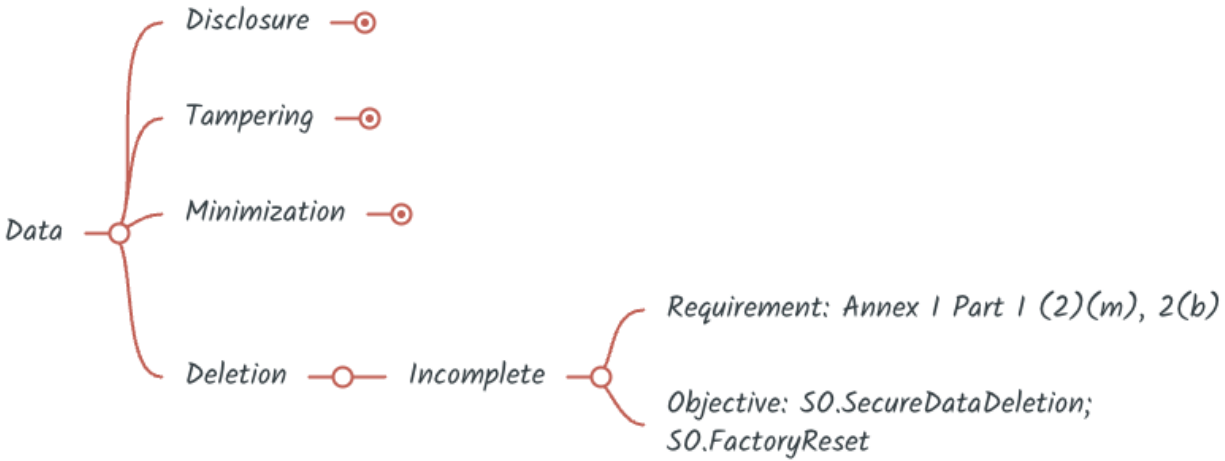
Recitals

- N/A

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.



- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

2.1. Article 3(3), point (d), of Directive 2014/53/EU

- ❑ -

2.2. Article 3(3), point (e), of Directive 2014/53/EU

- ❑ (g) allow users **to easily delete their stored personal data**, enabling the disposal or replacement of equipment without the risk of exposing personal data;

2.3. Article 3(3), point (f), of Directive 2014/53/EU

- ❑ -

GAP:
- Missing the deletion of data in general and in settings, not just personal data.
- ETSI EN 303 645 V3.1.3 – **Provision**: 5.11 Make it easy for users to delete user data

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

Threat	Security Objective
Threat.DeletedDataDisclosure	SO.SecureDataDeletion
Refer to ECR ANNEX I Part I (2) (e) of (EU) 2024/2847 Threat.DataInTransitDisclosure	SO.DataTransmittedConfidentiality SO.ComAuth
Refer to ECR ANNEX I Part I (2) (f) of (EU) 2024/2847 Threat.DataInTransitTampering	SO.DataTransmittedIntegrity SO.ComAuth

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

Mapping with 18031-X:2024

[DLM] Deletion mechanism
- [DLM-1] Applicability of deletion mechanisms

Added security controls

[DLM] Deletion mechanism
- [DLM-2] Confidential export of user data
- [DLM-3] Integrity protected of exported data
- [DLM-4] Authenticity of the communication partner for export of data

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

Think tank exercise on what could be required

- ❑ Provide a way to delete also the data stored in the “RDPS” and associated services (eg. Mobile application) beyond the product itself
- ❑ Robust erasure mechanisms (eg. Cryptographic erasure or multi-pass overwriting)
- ❑ Well-documented way to erase on a permanent bases of the data and settings
- ❑ Offer a way for the user to back up information and transfer it to another product if applicable
- ❑ Clearly communicate to the user the scope of the deletion and the effect
- ❑ Make sure that only authorized users can proceed into permanent deletion of data and settings

EXAMPLE OF REFERENCES –
- NIST SP 800-88 Rev. 2 - Guidelines for Media Sanitization
- ISO 27040:2024 Media Sanitization Requirements for Storage Sanitization
- ETSI 303 645 - 5.11 Make it easy for users to delete user data

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

How is 62443-4-2 approaching it?

- CR 4.2 – Information persistence
  - CR 4.2 RE (1) – Erase of shared memory resources
  - CR 4.2 RE (2) – Erase verification
- CR 4.3 – Use of cryptography
- CR 7.3 – Control system backup
- CR 7.4 – Control system recovery and reconstitution

- Vulnerability Assessment
- Secure Configuration
- Security updates
- Authorized access
- Confidentiality
- Integrity
- Data minimization
- Availability
- Minimize negative impact
- Attack surface minimization
- Incident impact reduction
- Logging and monitoring
- Secure deletion

ECR ANNEX I Part I (2) (m) - Data Deletion

(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.

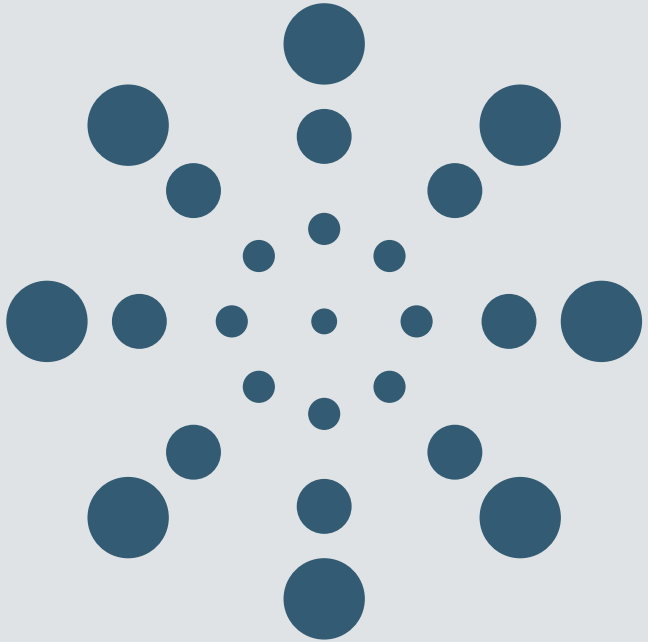
Security Objective	Technical Controls
SO.SecureDataDeletion	**[DLM] Deletion mechanism** (EN 18031) • [DLM-1] Applicability of deletion mechanisms (EN 18031)
ANNEX I Part I (2) (e) of (EU) 2024/2847 **SO.DataTransmittedConfidentiality**	**[DLM] Deletion mechanism** (EN 18031) • [DLM-2] Confidential export of user data (NEW)
ANNEX I Part I (2) (e)(f) of (EU) 2024/2847 **SO.ComAuth**	**[DLM] Deletion mechanism** (EN 18031) • [DLM-4] Authenticity of the communication partner for export of data (NEW)
ANNEX I Part I (2) (f) of (EU) 2024/2847 **SO.DataTransmittedIntegrity**	**[DLM] Deletion mechanism** (EN 18031) • [DLM-3] Integrity protected of exported data (NEW)

Survey (m)

- You are invited to answer this section of the survey
- Survey [LINK]

05

Conclusion



Post-Workshop Survey: Deep Dive Session Security Controls

- You are invited to answer this section of the survey
- Survey [LINK]
- Will remain open until 10 March 2026
- Report compiled with all the answers will be published in an aggregated and anonymous way (HERE)

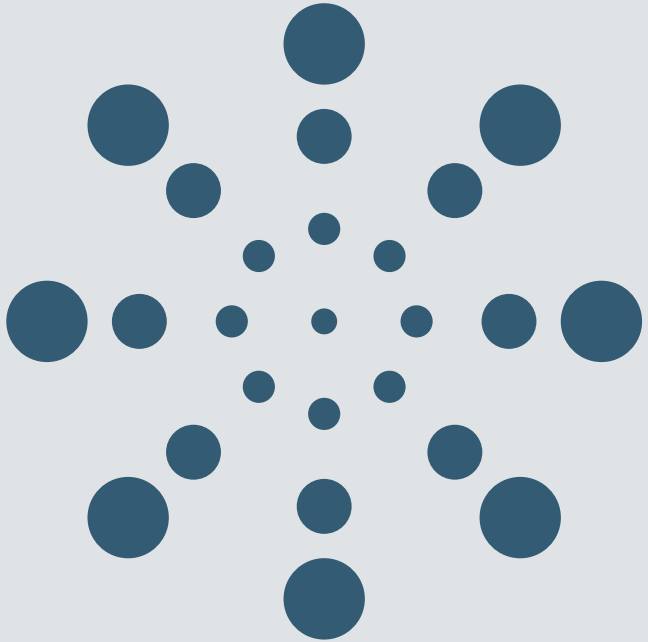
Vulnir

Thank you

VULNIR.com

info@vulnir.com

Mapping with ESR



ANNEX ZA: Overview of the ESR covered

(a) **be made available on the market without known exploitable vulnerabilities;**	– **Covered by** – GEC-1
(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 product with digital elements, including the possibility to reset the product to its original state;**	– **Covered by** – GEC-2 – GEC-3 – GEC-4 – GEC-5 – GEC-7 – GEC-9 – GEC-10 – GEC-12 – AUM-5 – DLM-1
(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;**	– **Covered by** – SUM-1 – SUM-2 – SUM-3 – SUM-4 – UNM-4
(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;**	– **Covered by** – ACM-1 – ACM-2 – AUM-1 – AUM-2 – AUM-3 – AUM-4 – AUM-5 – AUM-6 – GEC-13

ANNEX ZA: Overview of the ESR covered

(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;**	– **Covered by** – SSM-1 – SSM-3 – SCM-3 – SCM-2 – SCM-3 – SCM-4 – CCK-1 - CCK-2 – CCK-3 – CRY-1 – GEC-8
(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;**	– **Covered by** – SSM-1 – SCM-2 – SCM-3 – GEC-8 – GEC-13
(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 product with digital elements (data minimisation);**	– **Covered by** – UNM-1 – UNM-2 – DTM-1 – DTM-2 – DTM-3
(h) **protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;**	– **Covered by** – RLM-1 – RLM-2 – RLM-3 – RLM-4 – RLM-5 – RLM-6

ANNEX ZA: Overview of the ESR covered

(i) **minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;**	– **Covered by** – GEC-8 – TCM-1 – NMM-1 – LIM-1 – LIM-2
(j) **be designed, developed and produced to limit attack surfaces, including external interfaces;**	– **Covered by** – GEC-2 – GEC-3 – GEC-4 – GEC-5 – GEC-6 – GEC-7 – GEC-12
(k) **be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;**	– **Covered by** – GEC-11
(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;**	– **Covered by** – LGM-1 – LGM-2 – LGM-3 – LGM-4 – LGM-5 – LGM-6 – NMM-1 – MON-1 – MON-2

ANNEX ZA: Overview of the ESR covered

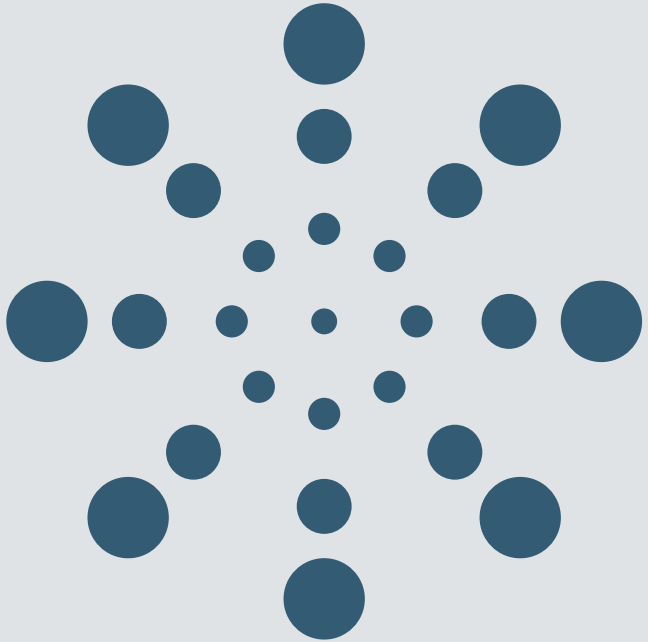
(m) **provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.**	– **Covered by** – [DLM-1] – [DLM-2] – [DLM-3] – [DLM-4]

Some refencences

- **Information Security Management**
  - ISO/IEC 27001, ISO/IEC 27002
- **Product and System Specific Security Requirements**
  - ETSI EN 303 645
  - EN IEC 62443-4-2
  - EN 18031-1, EN 18031-2, EN 18031-3
- **Security Evaluation and Testing**
  - ISO/IEC 18045
  - EN 17640
  - EN 17927
- **IoT Specifics (Architecture and Overarching Security)**
  - ISO/IEC 30141
  - ISO/IEC 27400
- **Privacy assurance**
  - ETSI TS 103 485
  - ISO/IEC 27400
  - ISO/IEC 27003
- **Security Throughout the Product Lifecycle**
  - ISO/IEC TR 6114

PT2 Outline

NOTE: Subject to change
Shared only for reference purposes



OUTLINE PT2 - Security controls (1 of 5)

- **7** **Technical Controls**
- **7.1** **[ACM] Access control mechanism**
- 7.1.1 [ACM-1] Applicability of access control mechanisms (EN 18031) (VOID)
- 7.1.2 [ACM-2] Access control mechanisms (Appropriate access control mechanisms)(EN 18031) (MERGE ACM-1 ACM2)
- **7.2** **[AUM] Authentication mechanism**
- 7.2.1 [AUM-1] Applicability of authentication mechanisms (EN 18031) (VOID)
- 7.2.2 [AUM-2] Appropriate authentication mechanisms (EN 18031)
- 7.2.3 [AUM-3] Authenticator validation (EN 18031)
- 7.2.4 [AUM-4] Changing authenticators (EN 18031)
- 7.2.5 [AUM-5] Password strength (EN 18031)
- 7.2.6 [AUM-6] Brute force protection (EN 18031)
- **7.3** **[SUM] Secure Update Mechanism (M43 - Round 1 - EN 18031)**
- 7.3.1 [SUM-1] Applicability of update mechanisms (EN 18031)
- 7.3.2 [SUM-2] Secure updates (EN 18031)
- 7.3.3 [SUM-3] Automated updates (EN 18031)
- 7.3.4 [SUM-4] Postponed Updates (NEW)
- **7.4** **[SSM] Secure storage mechanism (EN 18031)**
- 7.4.1 [SSM-1] Applicability of secure storage mechanisms (EN 18031)
- 7.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms (EN 18031)
- 7.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms (EN 18031)
- **7.5** **[SCM] Secure communication mechanism**
- 7.5.1 [SCM-1] Applicability of secure communication mechanisms (EN 18031) VOID
- 7.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms (EN 18031)

OUTLINE PT2 - Security controls (2 of 5)

- **7.5 [SCM] Secure communication mechanism**
- 7.5.1 [SCM-1] Applicability of secure communication mechanisms (EN 18031) VOID
- 7.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms (EN 18031)
- 7.5.3 [SCM-3] Secure communication mechanisms with confidentiality protection (EN 18031)
- 7.5.4 [SCM-4] Replay protection for secure communication mechanisms (EN 18031)
- **7.6 [LGM] Logging mechanism (18031)**
- 7.6.1 [LGM-1] Applicability of logging mechanisms (18031)
- 7.6.2 [LGM-2] Persistent storage of log data (18031)
- 7.6.3 [LGM-3] Minimum number of persistently stored events (18031)
- 7.6.4 [LGM-4] Time-related information of persistently stored log data (18031)
- 7.6.5 [LGM-5] Disabling logging (NEW)
- 7.6.6 [LGM-6] Exclude sensitive personal information (NEW)
- **7.7 [DLM] Deletion mechanism (EN 18031)**
- 7.7.1 [DLM-1] Secure Data deletion mechanisms (Applicability of deletion mechanisms) (EN 18031)
- 7.7.2 [DLM-2] Confidential export of user data (NEW)
- 7.7.3 [DLM-3] Integrity protected of exported data (NEW)
- 7.7.4 [DLM-4] Authenticity of the communication partner for export of data (NEW)
- **7.8 [UNM] User notification mechanism**
- 7.8.1 [UNM-1] Applicability of user notification mechanisms (EN 18031-2)
- 7.8.2 [UNM-2] Appropriate user notification content (EN 18031-2)
- 7.8.3 [UNM-3] User notification about detected anomalies (NEW) - (To be verified)
- 7.8.4 [UNM-4] User Security Update Notifications (NEW) - (To be verified)
-

OUTLINE PT2 - Security controls (3 of 5)

- **7.9** **[RLM] Resilience mechanism**
- 7.9.1 [RLM-1] Applicability and appropriateness of resilience mechanisms (EN 18031)
- 7.9.2 [RLM-2] Resilience - Recovery from incidents (NEW)
- 7.9.3 [RLM-3] Network prioritization (NEW)
- 7.9.4 [RLM-4] Resource prioritization (NEW)
- 7.9.5 [RLM-5] Resource management (NEW)
- 7.9.6 [RLM-6] Control system backup(NEW)
- **7.10** **[NMM] Network monitoring mechanism (EN 18031)**
- 7.10.1 [NMM-1] Applicability and appropriateness of network monitoring mechanisms (EN 18031)
- **7.11** **[TCM] Traffic control mechanism (EN 18031)**
- 7.11.1 [TCM-1] Applicability of and appropriate traffic control mechanisms (EN 18031)
- **7.12** **[CCK] Confidential cryptographic keys**
- 7.12.1 [CCK-1] Appropriate CCKs (EN 18031)
- 7.12.2 [CCK-2] CCK generation mechanisms (EN 18031)
- 7.12.3 [CCK-3] Preventing static default values for preinstalled CCKs (EN 18031)

OUTLINE PT2 - Security controls (4 of 5)

- **7.13 [GEC] General Equipment Capabilities**
- 7.13.1 [GEC-1] Up-to-date software and hardware ~~without known~~ exploitable vulnerabilities (EN 18031)
- 7.13.2 [GEC-2] Limit exposure of services via related network interfaces (EN 18031)
- 7.13.3 [GEC-3] Configuration of optional services and the related exposed network interfaces (EN 18031)
- 7.13.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces (EN 18031)
- 7.13.5 [GEC-5] No unnecessary external interfaces (EN 18031)
- 7.13.6 [GEC-6] Input validation (EN 18031)
- 7.13.7 [GEC-7] Documentation of external sensing capabilities (EN 18031)
- 7.13.8 [GEC-8] Product Integrity (EN 18031)
- 7.13.9 [GEC-9] Secure startup configuration (NEW)
- 7.13.10 [GEC-10] Factory Reset (NEW)
- 7.13.11 [GEC-11] Exploit mitigation mechanisms (NEW)
- 7.13.12 [GEC-12] No Unneeded Software Components (NEW)
- 7.13.13 [GEC-13] Report on possible unauthorised access and corruption (NEW)

OUTLINE PT2 - Security controls (5 of 5)

- **7.14 [CRY] Cryptography**
- 7.14.1 [CRY-1] Best practice cryptography (EN 18031)
- **7.15 [DTM] Data minimization**
- 7.15.1 [DTM-1] Data minimisation in relation to intended purpose (NEW)
- 7.15.2 [DTM-2] Default Data Processing Minimisation (NEW)
- 7.15.3 [DTM-3] Configurable Controls for Optional Data Processing (NEW)
- **7.16 [LIM] External impact limitation (NEW)**
- 7.16.1 [LIM-1] External impact limitation (NEW)
- 7.16.2 [LIM-2] Prevention of attack propagation (NEW)
- **7.17 [MON] Monitoring of security activities (NEW)**
- 7.17.1 [MON-1] Monitor security relevant activities (NEW)
- 7.17.2 [MON-2] Disable monitoring (NEW)

Vulnir.com
info@vulnir.com