Vulnir

Workshop: Cyber Resilience Act and Horizontal Standards

23rd September 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 (e.g., UL 2900, Common Criteria)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur (*) for CRA as a CEN contractor within CEN/CLC/JTC 13/WG 9 for
  - PT2: Generic Security Requirements
  - PT3: Vulnerability handling requirements

* 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.

Agenda

01 Setting up the context

02 CRA's use cases and examples

03 Security Controls Framework

04 Product-related Essential Requirements overview

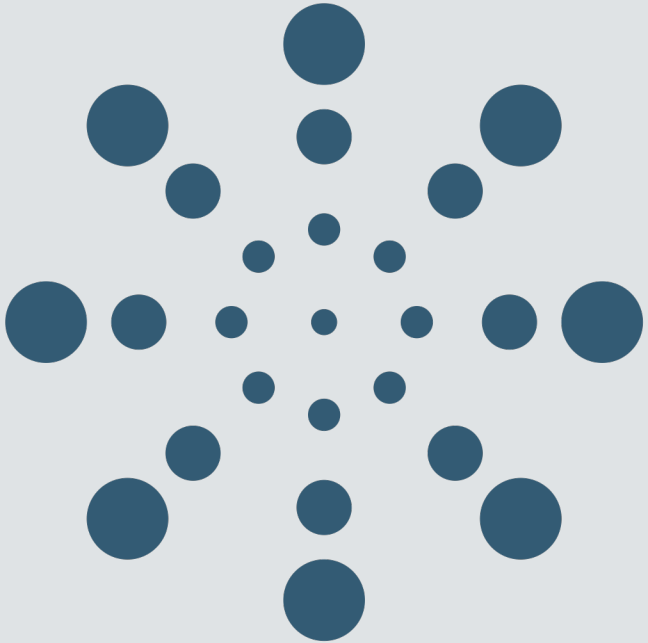
05 Status and Next Steps

06 Preparation / Workshop: Cyber Resilience Act and Horizontal Standards

01

Setting up the context

Preliminary knowledge useful for the workshop



How 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)

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

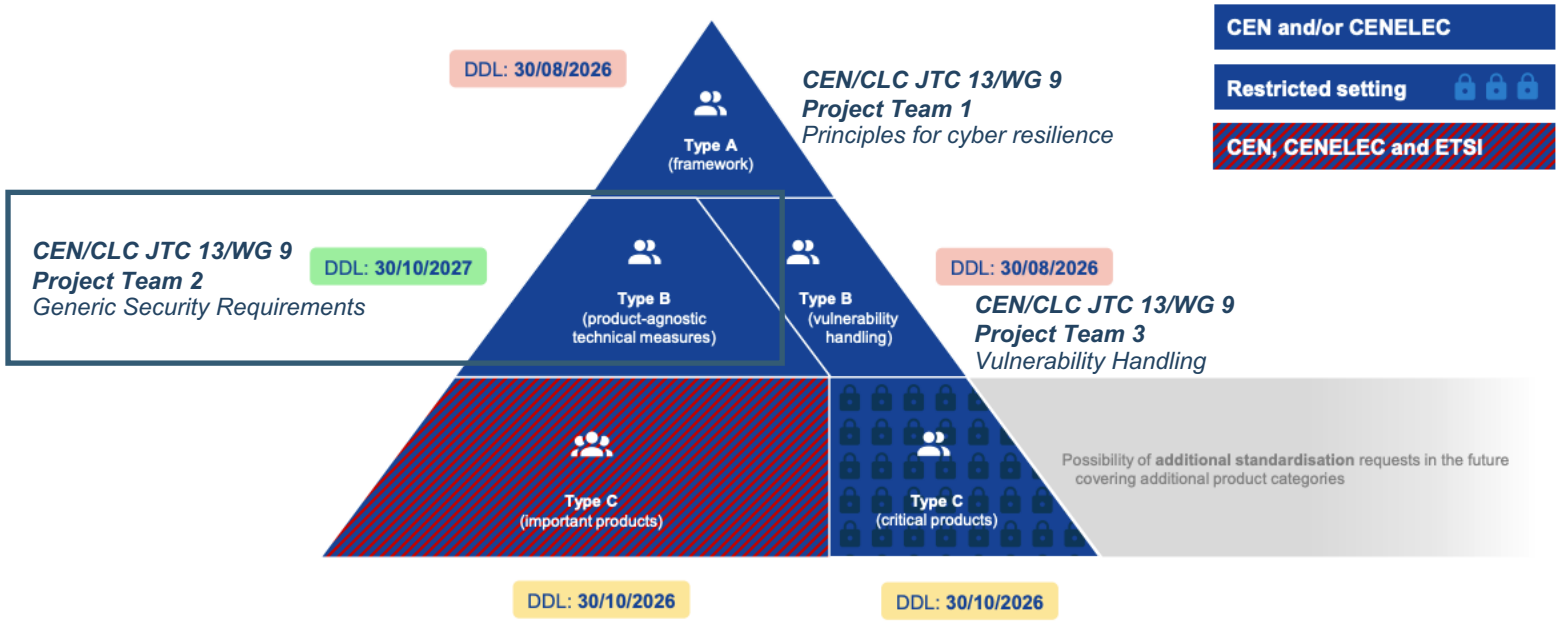
Maintenance

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

CRA standardisation request in a nutshell



European Commission

Source: Webinar on 26 February 2025 – Co-organised by Cyberstand.eu, HSbooster.eu & Stan4CR [The Cyber Resilience Act and where we stand]

Reference: CEN, CENELEC and ETSI Work Programme - Version: V 0.1 - Date: 2025-04-01 – **source:** [CYBERSTAND].

ANNEX I

List of new European Standards to be drafted

	Reference information	Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
1.	European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
2.	European standard(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027
4.	European standard(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30/10/2027
5.	European standard(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30/10/2027
6.	European standard(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30/10/2027
7.	European standard(s) on protecting the integrity of data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorised by the user, as well as reporting on corruptions	30/10/2027
8.	European standard(s) on processing only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements ('minimisation of data')	
9.	European standard(s) on protecting the availability of essential and basic functions of the product with digital elements	30/10/2027
10.	European standard(s) on minimising the negative impact of a product with digital elements or its connected devices on the availability of services provided by other devices or networks	30/10/2027
11.	European standard(s) on designing, developing and producing products with digital elements with limitted attack surfaces	30/10/2027
12.	European standard(s) on designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	30/10/2027
13.	European standard(s) on providing security related information by recording and/or monitoring relevant internal activity of products with digital elements with an opt-out mechanism for the user	30/10/2027
14.	European standard(s) on securely and easily removing or transferring all data and settings of a product with digital elements.	30/10/2027
Horizontal standards for vulnerability handling requirements		
15.	European standard(s) on vulnerability handling for products with digital elements	30/08/2026

❑PT1

❑PT2

❑PT3

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

Interplay between the three deliverables

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

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

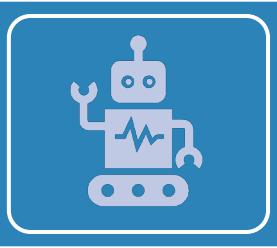
Project 2
A mapping of the essential product requirements to a list of appropriate **security controls** at various levels (controls have their own scale/levels to achieve the goal of the security control)

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

Main objectives of the deliverables

PT1: 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



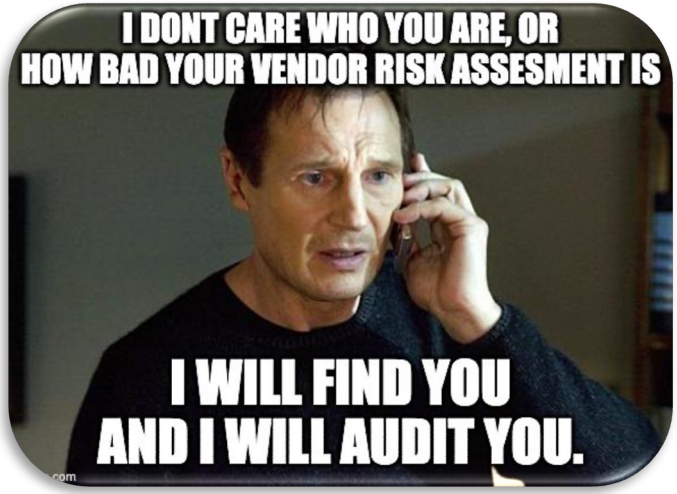
PT2: Generic security requirements

- 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

PT3: 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.)

Role of harmonised standards



Manufacturer

Can use it to demonstrate that their products meet the necessary requirements, thus facilitating market access.

Notified Bodies

Can use it to execute conformity assessment activities and verify the due diligence of the manufacturers that requested their services.

Harmonised standard: translates the legal requirement (what) to detailed technical requirements (how)

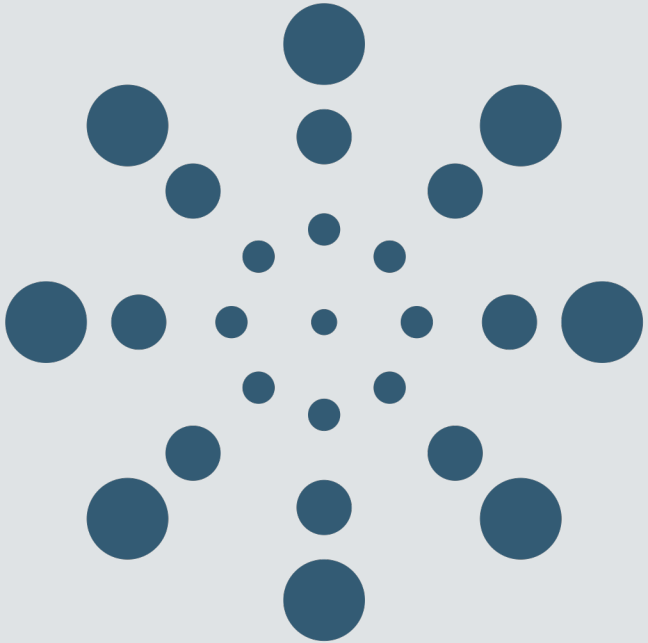
Can be used to verify consistently the implementation of an essential requirement

Market Surveillance

02

CRA

Use cases and examples



My Friend Cayla

- My Friend Cayla is made by Genesis Toys and distributed in Europe by Vivid Toy Group.
- The doll was named 2014 Innovative Toy of the Year by the London Toy Industry Association.
- The first vulnerability was disclosed in January 2015.
- In February 2017, the German Federal Network Agency (Bundesnetzagentur) had to invoke a federal law against espionage devices to ban a connected toy that intentionally transferred recordings outside the EU.

Source: https://www.npr.org/sections/alltechconsidered/2016/12/20/506208146/this-doll-may-be-recording-what-children-say-privacy-groups-charge (2016)

Issues and ESR violations

- **Lack of safety**: It was possible to talk and listen through the toy without requiring physical access to it. The problem stemmed from the design of the pairing.
  - Secure by default configuration
  - Authorized access
- **Illegal user terms**: The dolls could record and collect the private conversations of young children without any limitations on collection, use, or disclosure of this personal information.
  - Data minimization
- **Kids' secrets are shared:** Anything the child tells the doll is transferred to the U.S.-based company Nuance Communications, which specializes in speech recognition technologies.
- **Kids are subject to hidden marketing:** The toys are embedded with pre-programmed phrases that endorse different commercial products. For example, Cayla will happily talk about how much she loves different Disney movies; meanwhile, the app provider has a commercial relationship with Disney.

Role of essential requirements

Mirai IoT Botnet, Aug 2016

- The first ever botnet of Internet of Things devices
- **Root causes**:
  - Weak default configuration (default password)
- **Effect:**
  - High-profile websites and services that relied on Dyn for DNS resolution, including Twitter, Reddit, Netflix, Airbnb, Amazon were disrupted
- **Highlighted the importance of:**
  - Secure by default configuration

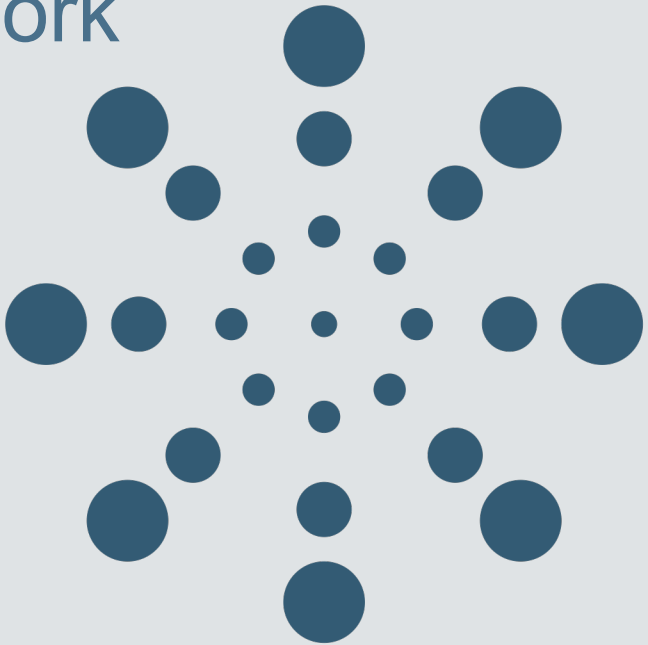
Log4j (Log4Shell), Dec 2021

- The first ever botnet of Internet of Things devices
- **Root cause**:
  - JNDI lookups within log messages without sufficient validation or sanitization
- **Effect:**
  - Its impact stemmed from the ubiquitous nature of the vulnerable Log4j library and the severe nature of the vulnerability itself (Remote Code Execution).
- **Highlighted the importance of:**
  - Security updates / SBOM

03

Security Controls Framework

Prepare

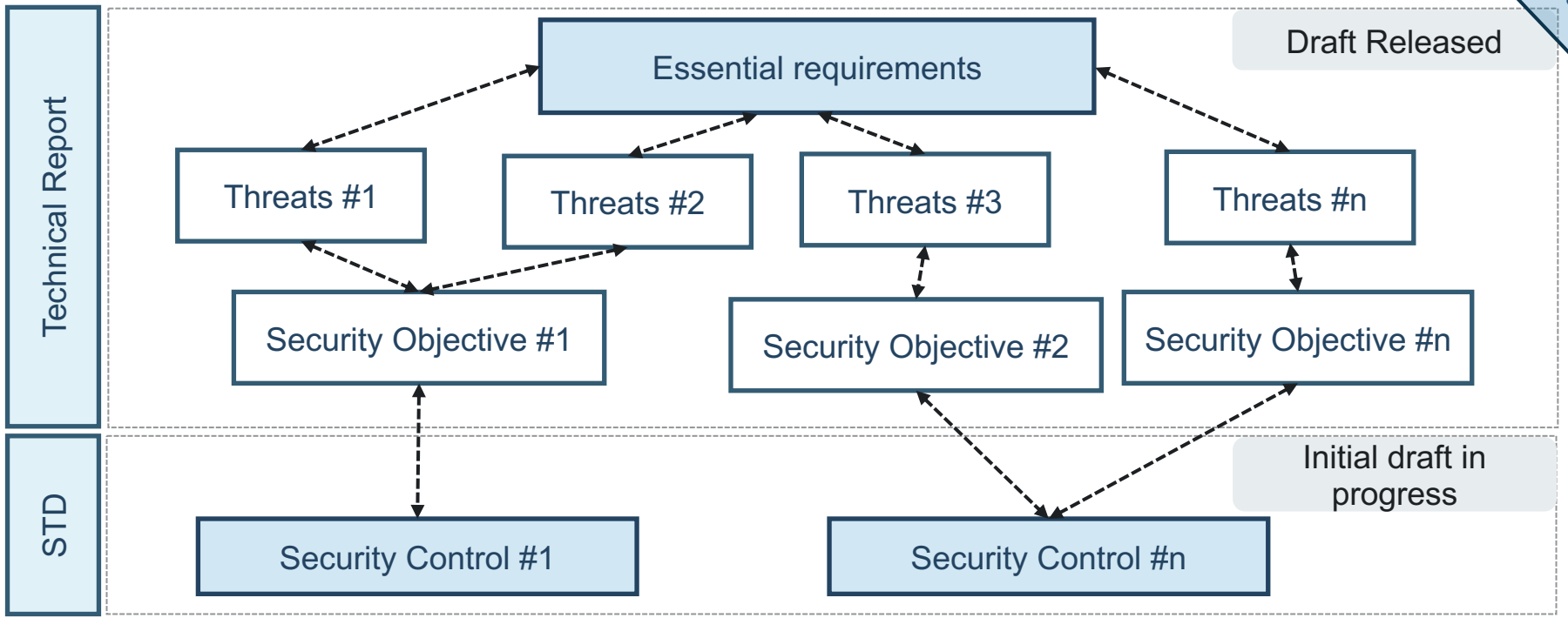


PT2 Objectives

- CRA requirement Annex I, Part I
- 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.
- Could be a guide for vertical standards and used as a reference
- Guide economic operators for products that fall into the default category
- Provides a library of security controls with their objectives and more technical assessment criteria
- Builds upon the EN 18031:2024 series, augmented with additional security controls
- 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.

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

PT2 Artifacts

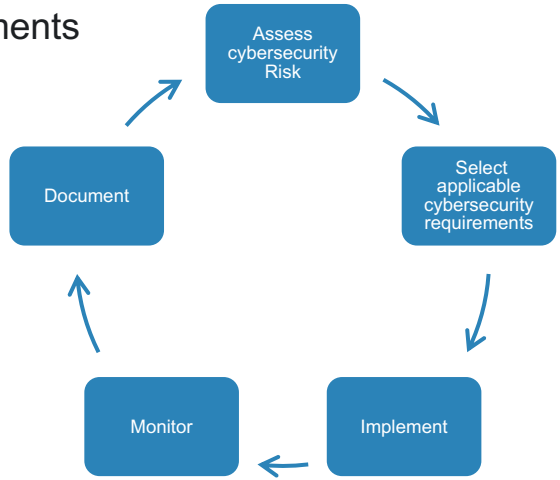


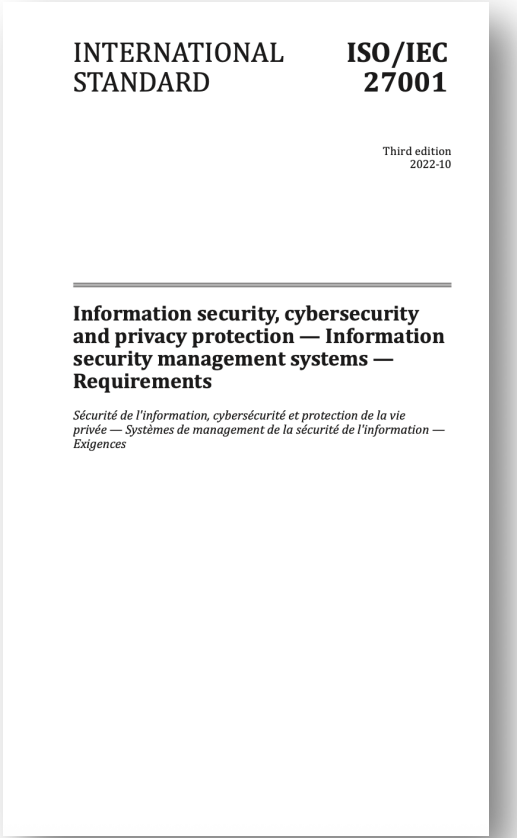
***Reference**: C(2025)618 – Standardisation request M/606*

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

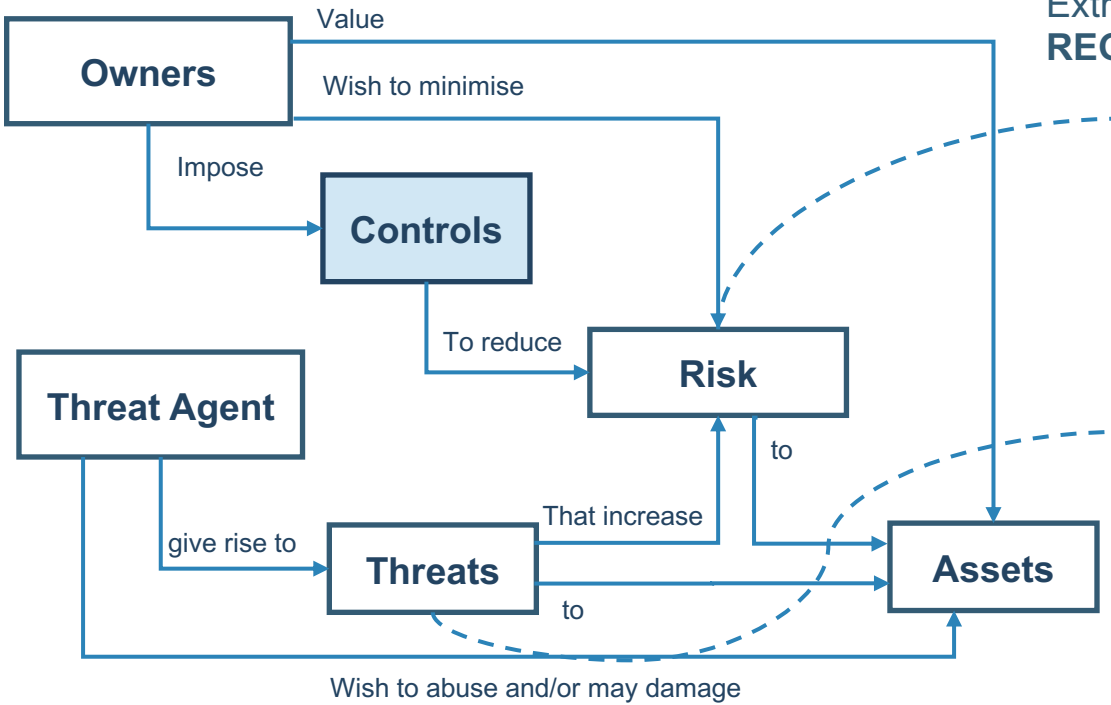
ISO/IEC 27001

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

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;

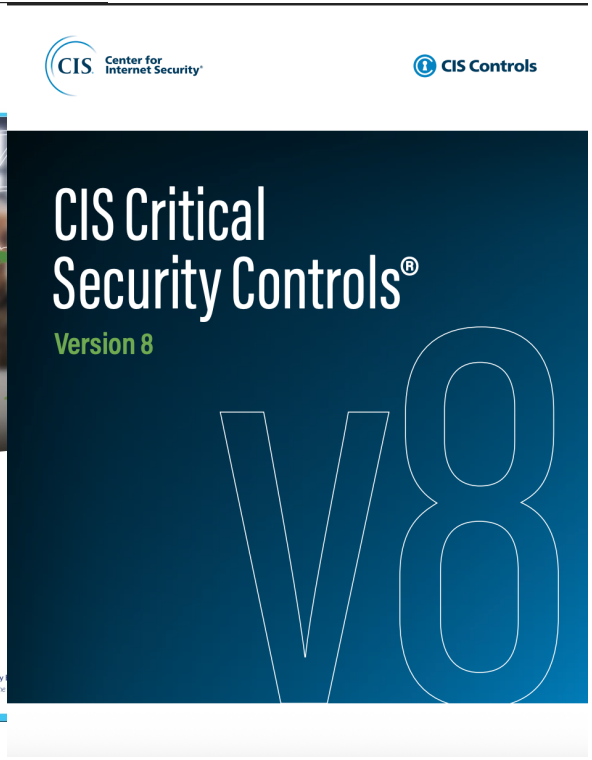
….

- (40) **'vulnerability'** means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat;

….

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

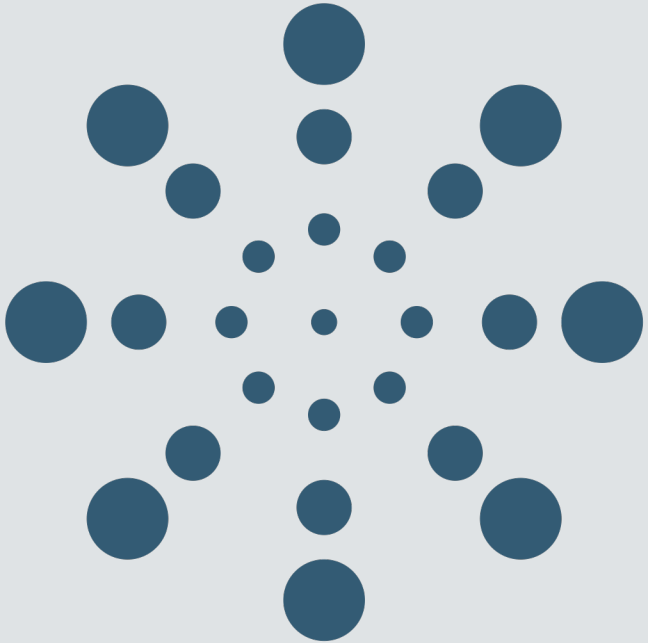
Example of security frameworks



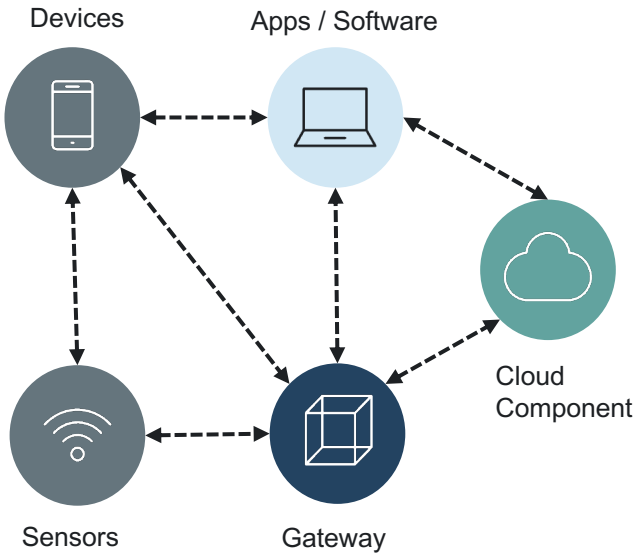
04

Essential Requirements

Understanding of the essential requirements and relevant implications



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

- 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 known exploitable vulnerabilities

ADDED SECURITY CONTROLS
NO ADDITION

Note:

- It is important to consider the process part (Vulnerability management activities) PT1/PT3
  - Test for known vulnerabilities
  - Regular tests that involves as minimum known vulnerabilities testing / vulnerability assessment
- Do we need a control/activity called **Known vulnerability assessment** with a focus on prioritizing weaknesses that are exploitable
- Considering if to include - **Threat.SupplyChainVulnerabilityExploitation**

- 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 SO.SecureStartupConfig
Threat.MissingResetFunctionalityConfigExploitation Threat.MissingResetFunctionalityMalwareExploitation Threat.MissingResetFunctionalityDataExtraction	SO.FactoryReset

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
  - OWASP Top 10 Proactive Controls - C5: Secure By Default Configurations
  - SA-8(23): Secure Defaults
- 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;

Mapping with 18031-X:2024

NO MAPPING

ADDED SECURITY CONTROLS

[GEC] General Equipment Capabilities

- [GEC-8] Secure default configuration
- [GEC-9] Secure startup configuration
- [GEC-10] Factory 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) (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 SO.AvailabilityOfUpdates:
Threat.UnpatchedVulnerabilityExploitation	SO.AutomaticUpdates SO.TimelyUpdates
Threat.MissingUpdateNotificationExploitation:	SO.UserUpdateNotification

Note/Challange:

- The challange is about the Remote Data Processing – could happen that manufacturers are using a silent patching approach for the “cloud component” side.
- How to deal with appropriate timeline and timely 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) (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] Availability of updates [SSU-2]
- [SUM-5] Update Mechanism [SSU-3]
- [SUM-6] Timely Updates [SSU-5]
- [SUM-7] User Update Notifications [SSU-6]
- [SUM-8] Postponed Updates [SSU-7]

- 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

Note:

- Missing control: additional **access control reporting**
  - (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;

Mapping with 18031-X:2024

[ACM] Access control mechanism

- [ACM-1] Applicability of access control mechanisms
- [ACM-2] Appropriate access control mechanisms

Mapping with 18031-X:2024

[AUM] Authentication mechanism

- [AUM-1] Applicability of authentication mechanisms
  - [AUM-1-1] Requirement network interface
  - [AUM-1-2] Requirement user interface
- [AUM-2] Appropriate authentication mechanisms
- [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

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;

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

Note:

- Missing control: requirements for protecting data in transit and processed

- 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) (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

Note:
- Missing control: requirements for protecting data processed

- 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] Secure communication mechanisms with integrity protection
- [SCM-2a] Secure communication mechanisms with authenticity protection

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) (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

Note:

- Still in definition phase and considering how to make it as a technical requirement and related to the capabilities of the products.
- It is clear that to minimize data relevant to support a functionality od specific use there should be a strong data classification process

- 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);

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 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) (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.LongTermAvailabilityDegradation	SO.IncidentRecovery
Threat.ShortTermAvailabilityDegradation	SO.IncidentResilience

Note:

- This requirement may be address by asking to the manufacturers to document the essential and basic functions and to define the related security controls
- Define and verity the fault tollerant mechanisms implemented from a product perespective if applicable

- 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] Resilience - Recovery from incidents

- 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) - External 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

Note:
- Still in definition phase in how to details this requirement from a product capability perspective

- 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) - External 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] Equipment Integrity

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) (j) - Attack Surface Minimization

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

Threat	Security Objective
Threat.UnnecessaryFunctionalityExploitation	SO.ReduceAttackSurface

Note:

- Still in definition phase but for sure we will include
  - hardening mechanisms
  - Documentation
  - Input 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) (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-11] Reduction of the attack surface

- 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) - Impact of Incident

(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:

- Still in definition phase: this requirement is clearly a process driven requirement but we will focus also in this case on the product capabilities and exploitation mitigation mechanisms and techniques. There is an overlap that need to be still formalize with the minimize negative impact

- 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) - Impact of Incident

(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-12] Reduction of the impact of an incident

- 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.SecurityActivitiesNotMonitoredRecorded	SO.DetectionOfSecurityRelevantActivities SO.InfoAboutSecurityRelevantActivities
Threat.MonitoringDataDisclosure	SO.OptionDisableDataMonitoring

Note:
- Still in definition phase

- 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

[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] Recording and monitoring of security activities
- [LGM-6] Monitoring of security relevant activities
- [LGM-7] Providing information about monitored activities
- [LGM-8] Disabling 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) (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
Threat.MissingDataRemovalExploitation	SO.SecureDisposalByUser
Threat.DataInTransitDisclosure	SO.SecureComConfidentiality SO.ComAuth
Threat.DataInTransitTampering:	SO.SecureComIntegrity: SO.ComAuth:

Note/challanges:

- How to take in consideration the data deletion for data in transit – this can be done on a communication level (SCM)
- Having a SO.ComAuth may be redundant or not contexualize for data deletion but of course you expect that only the authorized entity could execute this function

- 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

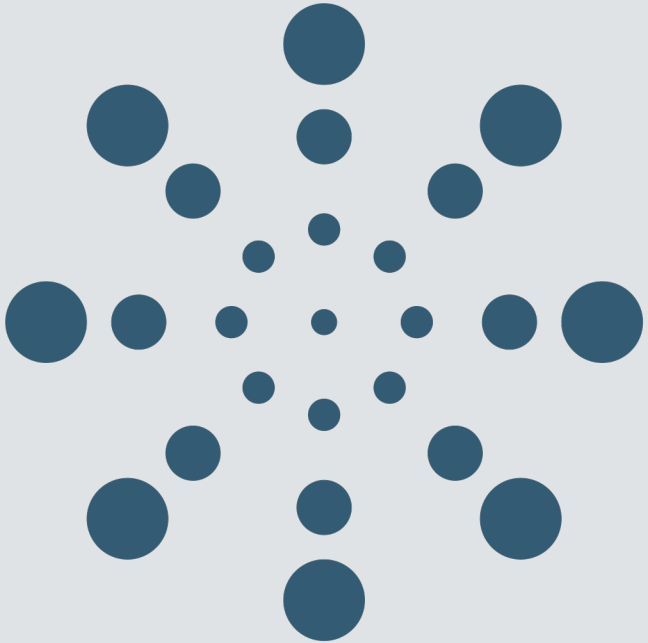
ADDED SECURITY CONTROLS

[DLM] Deletion mechanism
- [DLM-2] Secure data deletion
- [DLM-3] Secure disposal by the user [DEL-1]
- [DLM-4] Confidential export of deleted data
- [DLM-5] Authenticity of the communication partner for export of deleted data
- [DLM-6] Protection against leaking meta information
- [DLM-7] Integrity protected export of deleted data

05

Status and Next Steps

Status and next steps



Some refencences

- **ENISA**
  - EUCC SCHEME GUIDELINES ON VULNERABILITY MANAGEMENT AND DISCLOSURE, Version 1.1, January 2025
  - Vulnerability disclosure
    - https://www.enisa.europa.eu/topics/vulnerability-disclosure
- **IoT Security Foundation**
  - Vulnerability Disclosure, Best Practice Guidelines, Release 2.0, September 2021
- **FIRST**
  - Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Spring 2020
  - PSIRT Services Framework
- **NIST**
  - Vulnerability Disclosure Guidelines
    - https://csrc.nist.gov/Projects/vulnerability-disclosure-guidelines)
- **ETSI**
  - ETSI TR 103 838 V1.1.1 (2022-01) Cyber Security;Guide to Coordinated Vulnerability Disclosure
  - ETSI TR 104 003 V1.1.1 (2024-09) The vulnerability disclosure ecosystem
- **ISO/IEC**
  - ISO/IEC TR 5895:2022 - Cybersecurity — Multi-party coordinated vulnerability disclosure and handling
  - SO/IEC 30111:2019 - Information technology — Security techniques — Vulnerability handling processes
  - ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure
  - ISO/IEC 18974:2023 - Information technology — OpenChain security assurance specification
- **IoT Security Foundation**
  - The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2024 (25th November 2024)
- **Google**
  - Guide to coordinated vulnerability disclosure for open-source projects (https://github.com/google/oss-vulnerability-guide/tree/main)

Example standards with affinities with PT2 standard

- 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
- IoT Specifics (Architecture and Overarching Security)
  - ISO/IEC 30141
  - ISO/IEC 27400
- Privacy assurance
  - ETSI TS 103 485
- Security Throughout the Product Lifecycle
  - ISO/IEC TR 6114

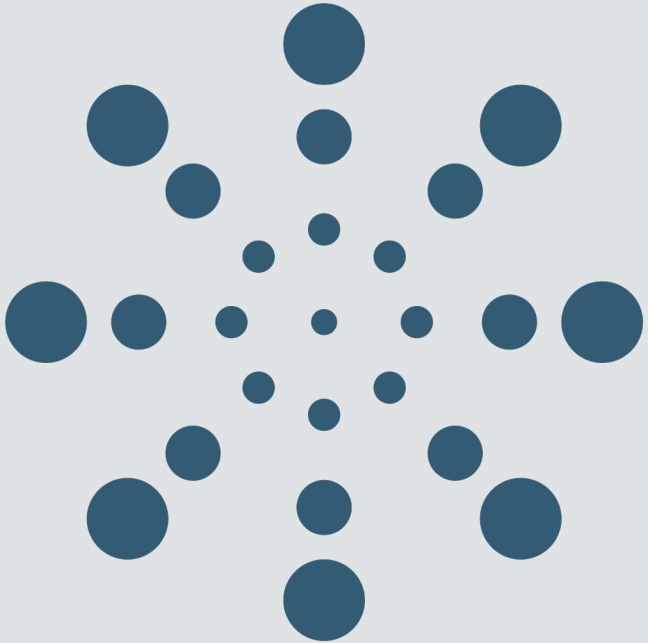
***NOTE**: This list is not exhaustive, but just a starting point for interesting references*

Next Steps

- We developed an initial Technical Report that links essential requirements, threats, and security objectives.
  - Validate the TR and identify any missing threats, given the horizontal nature of the PT2 standard.
  - An instantiation with a reference architecture and demonstrate the allocation of threats and their corresponding security controls, aligned with essential requirements from the CRA.
  - Propose a characterization of security controls and allocate to a use case (eg, IP camera, smart washing machine, or other)
- The PT2 standard is still in an early stage.
  - Bring to the table case studies and examples that we should consider when defining the security requirements and potential exceptions, if any.
  - Perspectives to support the definition of appropriate evaluation methodology for security controls
- For when we have a more complete PT2 draft.
  - It would be interesting to have a pilot evaluation of security controls for a use case (eg, IP camera, smart washing machine, or other)

06

Preparation / Workshop: Cyber Resilience Act and Horizontal Standards



Workshop Scenarios

SCENARIO 1 - CURRENT PRODUCT INTENDED ENVIROMENT

A **time switch** installed in office buildings is used to **control heating or air conditioning systems** based on programmed schedules to optimize energy consumption and comfort.

OBJECTIVE

Consider what activities a company like Dinuy (SME) needs to do in order to ensure that the time switch shall be designed, developed, produced, maintained, and disposed of in such a way that they ensure an appropriate level of cybersecurity based on the risks across the entire lifecycle of the product.

Consider at least the following:

- Risk assessment and treatment
- Essential Cybersecurity Requirements
- Communication with relevant stakeholders
- Updates - lifecycle
- Documentation


Nueva Gama de
Programadores Horarios sin pantalla
DiNUY
Brighten up your day.
Descargue aquí la APP
DINUY CONFIGURE
NIESSEN
DiNUY
IH PLA BW1
230V~ 50/60Hz
20:30

Product configuration process

Time Switch

DINUY-Configure App

First time after installing App:
Log in to the App or user register

Scan available devices

Available devices visible

Select device to configure

App reads PIN

User must enter PIN if activated (no PIN by defaut)

Configure programs and PIN (if new)

https://

Register user email (form)

Ask for ack by email

Send ack (validate user)

DINUY Cloud Server

Workshop input and activities

- **Presentation from Dinuy**: you will have the full presentation where the product (time-switch) including mobile and cloud will be presented along with product configuration, development process, risks assessment
- **Presentation on PT2 Security controls**: Presenting the security controls and workshop flows – mostly based on this material
- **Case Study Feedback:** we will ask to attendees to fill in some questionnaire to collect inputs in a structured way
- **What will happen**:
  1. There will be 10 coordinators assigned to 10 table onsite and each table will have assigned some risks to analize
  2. There will be 10 coordinators assigned to 10 breakout rooms online and each breakout rom will have assigned some risks to analyze
  3. The goal would be to analyze and assign the right security controls for the pre-assigned risk including writing down challenges and lesson learned
  4. Table coordinators will guide the attendees in moderating the discussion and fill in the Case Study Feedback
  5. The table coordinators will summarize the key points that will be then discussed in a closure session as a panel discussion

Table Mapping Assignment

CRA Workshop - TABLE and RISKS Assignment

Note: This table shows the pre-assigned risk distribution for the September 23rd CRA Workshop. Each table coordinator will focus on their assigned risks during the case study sessions (12:10-16:30).

Nº Table/Room	Gr.RISKS	RISK Descriptions	IN-PERSON	Participan	ONLINE Coordinator	Participants
TABLE/ROOM 1	RISK G1 & G6 (2)	RISK G1: Communication interception - MITM [SCM, CRY] RISK G6: Credential theft/misuse [SSM, CCK]	Miguel Bañon	see the page	David Arroyo	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 2	RISK G2 & G8 (2)	RISK G2: Unauthorized access [AUM, ACM, GEC] RISK G8: Lack of incident detection [NMM, MON]	Jesús Fernandez	see the page	Roger Riera Guardia	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 3	RISK G3 & G9 & g10 (3)	RISK G3: Unauthorized data access from storage [SSM, GEC] RISK G9: Tracking and targeting [GEC] RISK G10: Reverse engineering of app [SSM, GEC]	César de la Serna	see the page	Simon Dunkley	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 4	RISK G4 & G11 & G12 (3)	RISK G4: Brute force attack [ACM, GEC] RISK G11: Excess data collection [DLM, DTM] RISK G12: Denial of Service [NMM]	Constantinos Tsiourtos	see the page	Riccardo Sirigu	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 5	RISK G5 & G7 (2)	RISK G5: Malicious firmware installation [SUM, UNM, GEC] RISK G7: Compromise via outdated software [SUM, UNM, GEC]	Salvador Trujillo	see the page	Sebastien Viou	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 6	RISK G1 & G6 (2)	RISK G1: Communication interception - MITM [SCM, CRY] RISK G6: Credential theft/misuse [SSM, CCK]	Jesús Luna	see the page	Piet De Vaere	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 7	RISK G2 & G8 (2)	RISK G2: Unauthorized access [AUM, ACM, GEC] RISK G8: Lack of incident detection [NMM, MON]	Maria Raphael	see the page	José Capote	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 8	RISK G3 & G9 & G10 (3)	RISK G3: Unauthorized data access from storage [SSM, GEC] RISK G9: Tracking and targeting [GEC] RISK G10: Reverse engineering of app [SSM, GEC]	Tim Scherer	see the page	María-Amor Domínguez	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 9	RISK G4 & G11 & G12 (3)	RISK G4: Brute force attack [ACM, GEC] RISK G11: Excess data collection [DLM, DTM] RISK G12: Denial of Service [NMM]	Unai Gomez	see the page	Javier Augusto Gil-Ruiz Gil-Esparza	N/A. Online participants will be assigned RANDOMLY.
TABLE/ROOM 10	RISK G5 & G7 (2)	RISK G5: Malicious firmware installation [SUM, UNM, GEC] RISK G7: Compromise via outdated software [SUM, UNM, GEC]	Carlos Vives	see the page	Miguel Martín Redondo	N/A. Online participants will be assigned RANDOMLY.

Instructions for Coordinators:

1. Focus your onsite table (or online room)'s analysis on your assigned Group_Risks ONLY.
2. Guide participants of your table/room through the FEEDBACK SURVEY FORM for the mentioned specific risks, submit the form, the answers will automatically arrive to us.
3. Collect comprehensive inputs/feedback from your table/room participants to fill them into the FEEDBACK_SURVEY_FORM, and at the end of the workshop, submit the completed form to us.

TABLE+ROOM_RISKS_Coordinator_Participant_.xlsx

Table Mapping Assignment – Risk Groups

TABLES	Group_RISKS		RiskID				
T1, T6	RISK-G1: Communication interception - MITM [SCM, CRY]	1	RT1	Scheduling function	Bluetooth communication interception (MITM)	Unencrypted communication	
			RM4	Bluetooth communication channel	MITM over Bluetooth	Lack of secure pairing	
			RM5	User data handled by the app	Data interception in transmission	Absence of TLS Lack of cert validation	Use of TLS for https
			RM7	Cloud server and API endpoints	Data interception in transmission	Absence of TLS Lack of cert validation	Use of TLS for https
			RC1	User Form Data (Name, Email, etc.)	Data interception during submission	No TLS, invalid certificates	**OpenSSL**: Enforce TLS 1.3
T2, T7	RISK-G2: Unauthorized access [AUM, ACM, GEC]	2	RT2	On/Off control	Unauthorized access	Weak/No pairing keys	PIN control in App
			RT8	Configuration app	Social engineering	Lack of app access control	Option to limit Time switch access control with PIN
			RM3	Bluetooth communication channel	Unauthorized Bluetooth access	Lack of authentication and secure pairing	PIN control in App
			RM8	Cloud server and API endpoints	Unauthorized API access	Insecure API design Inadequate input validation	
			RC5	Email verification process	Spoofing of verification emails	Improper SPF/DKIM/DMARC setup	Use **SPF, DKIM, DMARC** with SMTP provider
			RC3	API endpoints (form submission, verification)	Unauthorized access attempts	Weak authentication, lack of filtering	**iptables, APF, ModSecurity, Fail2ban:** filter traffic and block brute force
			RC9	Cloud Server	Rootkit or malware persistence	Lack of detection tools	**LMD, rkhunter:** periodic scans
T3, T8	RISK-G3: Unauthorized data access from storage [SSM, GEC]	3	RM6	User data handled by the app	Unauthorized data access from storage	Unencrypted local data storage	PIN control in App
			RC2	User Form Data (Name, Email, etc.)	Unauthorized access to stored data	Misconfigured DB, weak permissions	**RBAC, DB hardening, encryption at rest**
T4, T9	RISK-G4: Brute force attack [ACM, GEC]	4	RT3	PIN configuration code	Brute force attack	Weak PIN length	App lockout after 6 attempts
			RT4	Master PIN code	Social engineering	Spoofed call to the factory	No static Master PIN code
T5, T10	RISK-G5: Malicious firmware installation	5	RT5	Device firmware	Malicious firmware installation	No integrity validation	FW update with encryption, firmware signature validation and secure keys if applied
	[SUM, UNM, GEC]		RM10	Firmware/Software Update Mechanism of the App	Malicious firmware/software update	Lack of update signing and verification	The app can be updated through the stores (Google Play/App Store). Use only official stores, secure developer accounts (double authentication + build certificate)
T1, T6	RISK-G6: Credential theft/misuse [SSM, CCK]	6	RT7	Pairing data	Key sniffing	Plaintext key storage	secure storage if applied
			RM9	Authentication credentials	Credential theft/misuse	Unencrypted storage Outdated libraries	Flutter_secure_storage (or a native equivalent) is currently being used.
			RC7	Database storing user form data	Data loss or corruption	No backups, no redundancy	Implement **regular backups, test recovery**
T5, T10	RISK-G7: Compromise via outdated software [SUM, UNM. GEC]	7	RM2	Mobile application code & configurations	Known flutter libraries threats	Outdated libraries	Flutter libraries updated with identified critical vulnerabilities
			RC8	Cloud Server	Compromise via outdated software	Unpatched services	Regular OS and service updates, kernel hardening
T2, T7	RISK-G8: Lack of incident detection [NMM, MON]	8	RM11	Logging & Monitoring	Lack of detection	No logging implemented	Local logs on the server
			RC11	Logging and Monitoring	Lack of incident detection	No log analysis or monitoring	**rsyslog, Logwatch:** enable log collection and daily analysis
T3, T8	RISK-G9: Tracking and targeting [GEC]	9	RT6	BLE network identifiers (name, UUID, MAC)	Tracking and targeting	Publicly visible identifiers	
T3, T8	RISK-G10: Reverse engineering of app [SSM, GEC]	10	RM1	Mobile application code & configurations	Reverse engineering of app	Insufficient app hardening	The Flutter app is compiled (Dart AOT). App is converted to native machine code before it runs
T4, T9	RISK-G11: Excess data collection [DLM, DTM]	11	RM12	Data management	excess data collection	No minimization controls	
			RC12	Decommissioning user data	Residual data post-deletion	No secure deletion policy	Implement secure wipe procedures
T4, T9	RISK-G12: Denial of Service [NMM]	12	RC4	API endpoints (form submission, verification)	Denial of Service	No rate limiting, no WAF	**ModSecurity (WAF), Fail2ban, iptables:** mitigate DoS
			RC6	Email verification process	User does not receive email	Delivery issues	Monitor delivery, retry logic
			RC10	Cloud Server	Spam from server	Uncontrolled mail flow	**SpamAssassin, SMTP rate limiting**

TABLE+ROOM_RISKS_Coordinator_Participant_Assignments.xlsx

Closure of the Dynamic-Workshop on Case Study

- **Presentation of the feedback form results**
  Presentation of the data from the Microsoft Form live to close the workshop
- **Presentation of onsite participants of their learnings and conclusions**
  Three representants of the three different onsite tables will present their findings, conclusions, and the difficulties they encountered throughout the dynamic-workshop case study

Q&A

Thank you

VULNIR.com

info@vulnir.com