Vulnir

Online CRA Workshop 'Deep dive session: Vulnerability Handling'

22 July 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 Product-related Essential Requirements overview

04 Vulnerability handling Essential Requirements overview

05 Vulnerability handling: Deep Dive

5.1 5.1 [PRE] PREPARATION

5.2 5.2 [RCP] RECEIPT

5.3 5.3 [VRF] VERIFICATION

5.4 5.4 [RMD] REMEDIATION

5.5 5.5 [RLS] RELEASE

5.6 5.6 [PRP] POST RELEASE

01

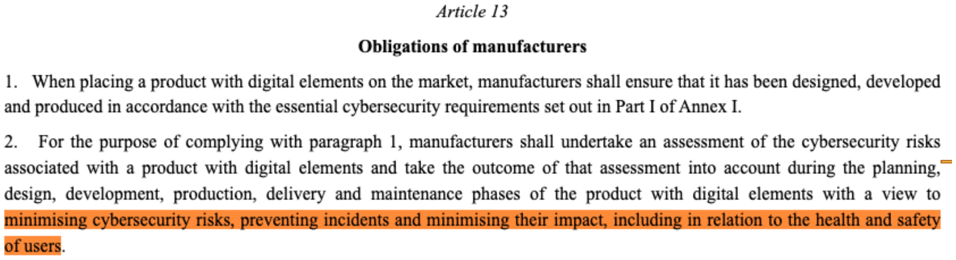
Setting up the context

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)

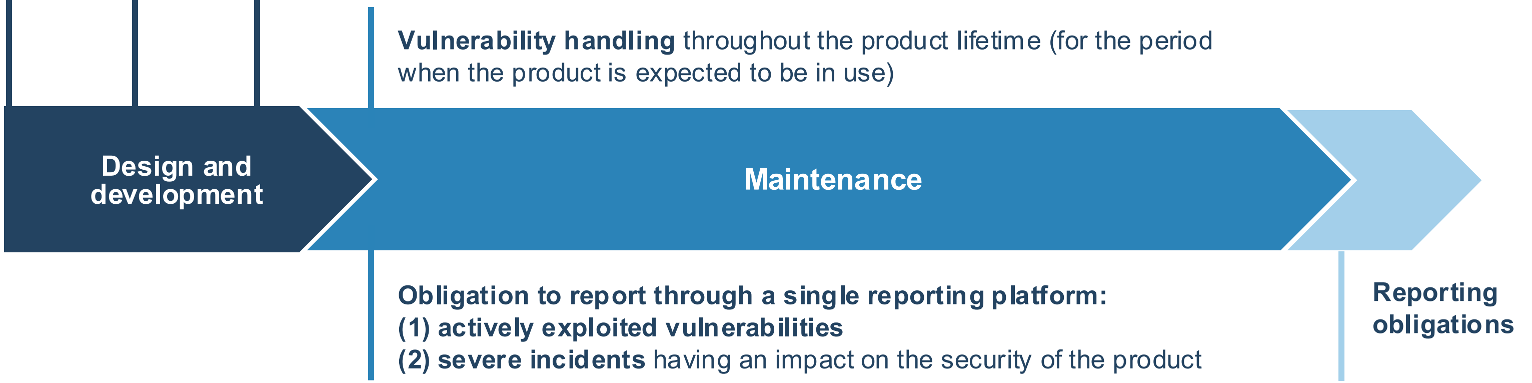


Article 13

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.



Risk Assessment

Product-related essential requirements

Vulnerability handling essential requirements

Conformity assessment

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

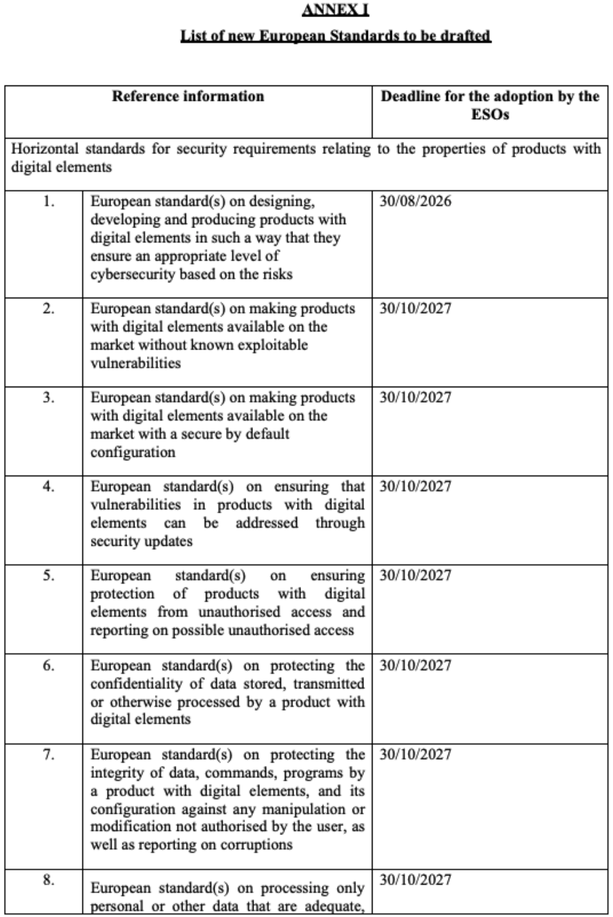
Design and development

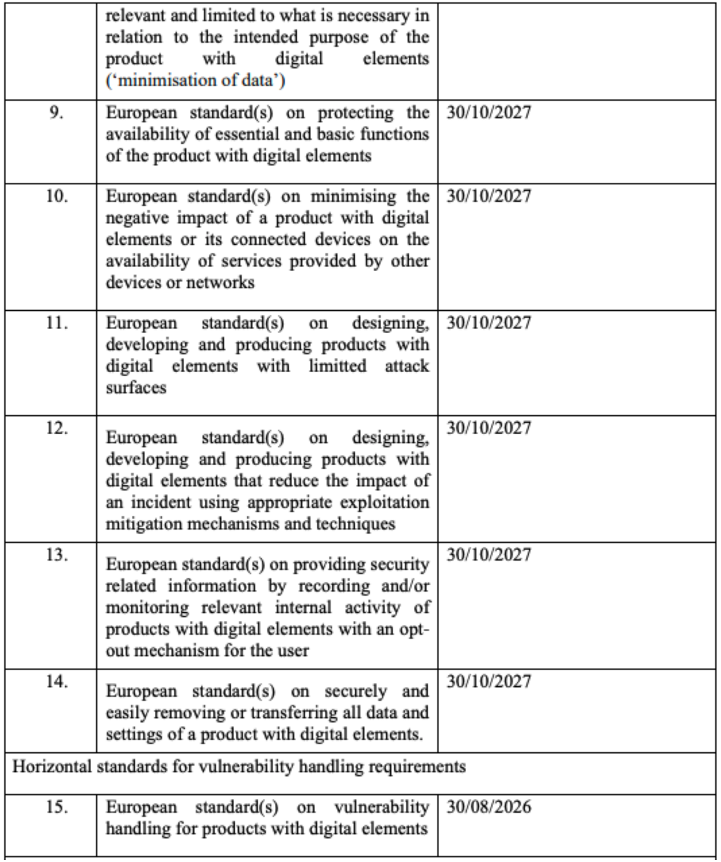
Maintenance

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*





ANNEX I

List of new European Standards to be drafted

❑PT1

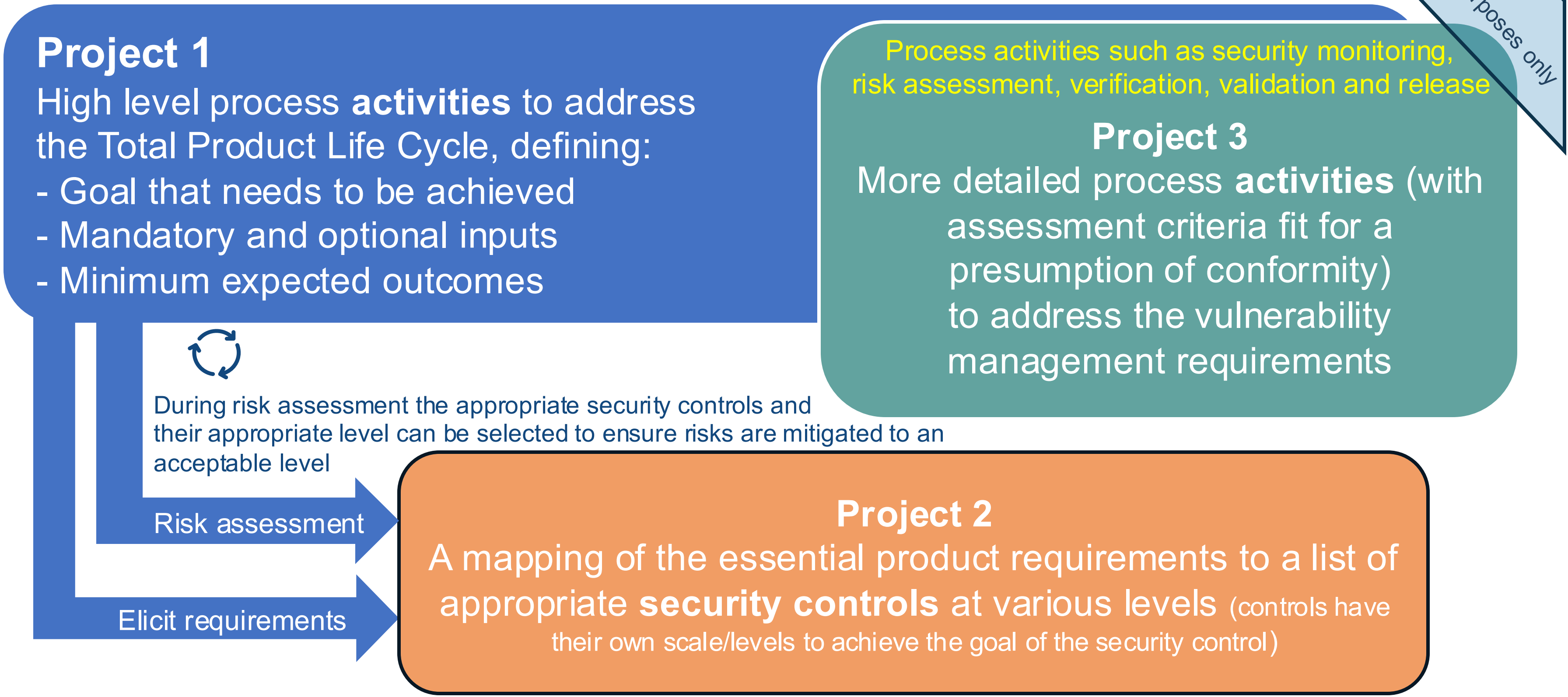
❑PT2

❑PT3

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')	30/10/2027
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

***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

I DONT CARE WHO YOU ARE, OR
HOW BAD YOUR VENDOR RISK ASSESMENT IS
I WILL FIND YOU
AND I WILL AUDIT YOU.

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

Vulnir

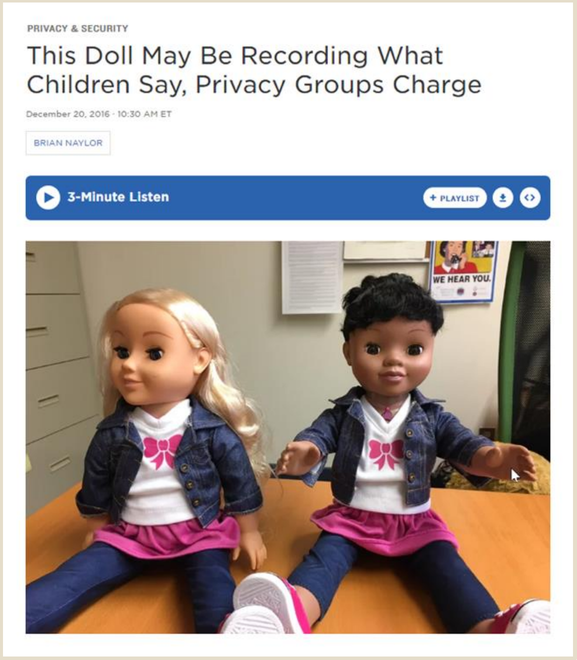
02

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.



PRIVACY & SECURITY

This Doll May Be Recording What Children Say, Privacy Groups Charge

December 20, 2016 · 10:30 AM ET

BRIAN NAYLOR

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.
- **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.
- **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.

- Secure by default configuration
- Authorized access
- Data minimization

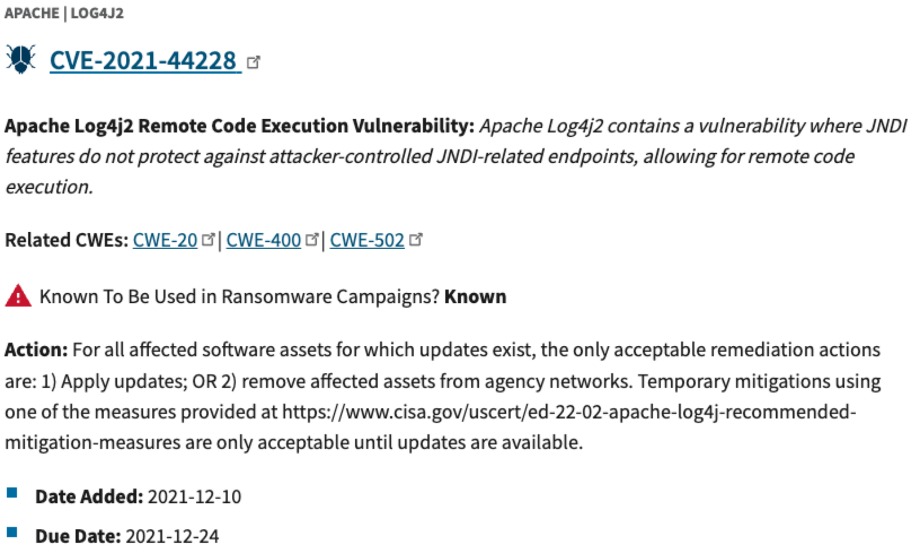
Role of essential requirements

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



APACHE | LOG4J2

CVE-2021-44228

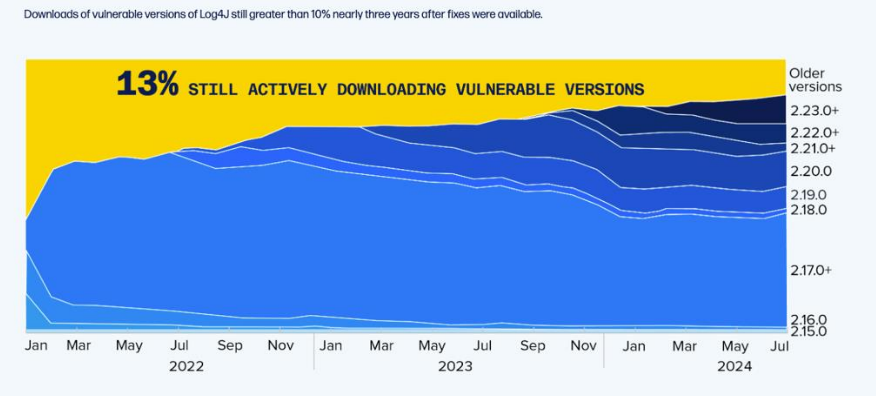
Apache Log4j2 Remote Code Execution Vulnerability: *Apache Log4j2 contains a vulnerability where JNDI features do not protect against attacker-controlled JNDI-related endpoints, allowing for remote code execution.*

Related CWEs: CWE-20 | CWE-400 | CWE-502

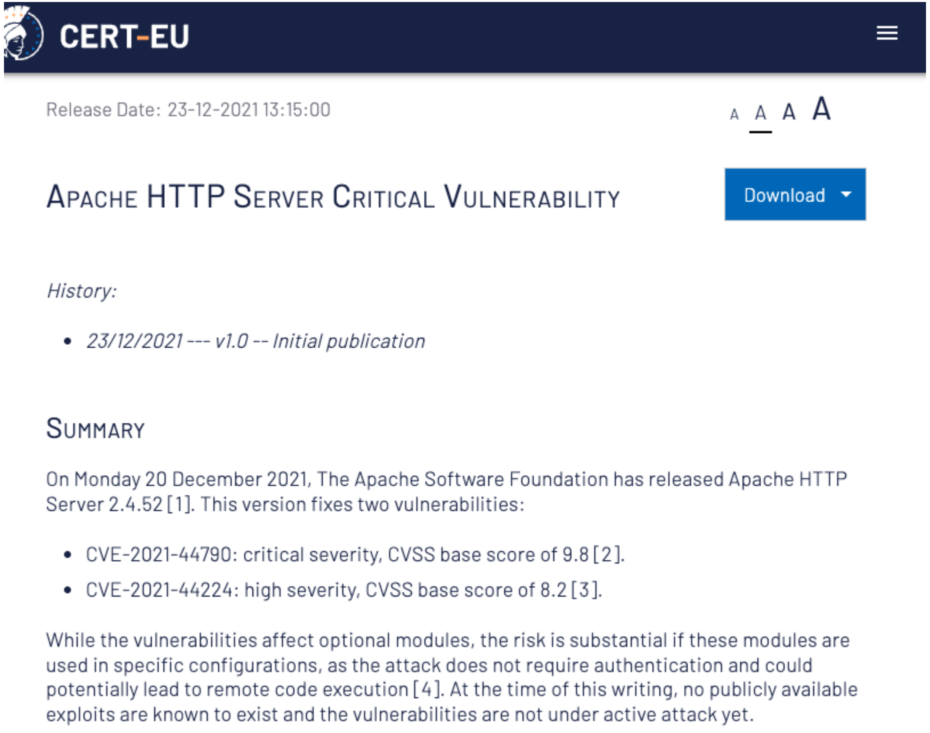
Known To Be Used in Ransomware Campaigns? **Known**

Action: For all affected software assets for which updates exist, the only acceptable remediation actions are: 1) Apply updates; OR 2) remove affected assets from agency networks. Temporary mitigations using one of the measures provided at https://www.cisa.gov/uscert/ed-22-02-apache-log4j-recommended-mitigation-measures are only acceptable until updates are available.

- **Date Added:** 2021-12-10
- **Due Date:** 2021-12-24



Downloads of vulnerable versions of Log4J still greater than 10% nearly three years after fixes were available.



Release Date: 23-12-2021 13:15:00

Apache HTTP Server Critical Vulnerability

History:

- *23/12/2021 --- v1.0 -- Initial publication*

Summary

On Monday 20 December 2021, The Apache Software Foundation has released Apache HTTP Server 2.4.52 [1]. This version fixes two vulnerabilities:

- CVE-2021-44790: critical severity, CVSS base score of 9.8 [2].
- CVE-2021-44224: high severity, CVSS base score of 8.2 [3].

While the vulnerabilities affect optional modules, the risk is substantial if these modules are used in specific configurations, as the attack does not require authentication and could potentially lead to remote code execution [4]. At the time of this writing, no publicly available exploits are known to exist and the vulnerabilities are not under active attack yet.

Source: https://www.sonatype.com/resources/log4j-vulnerability-resource-center

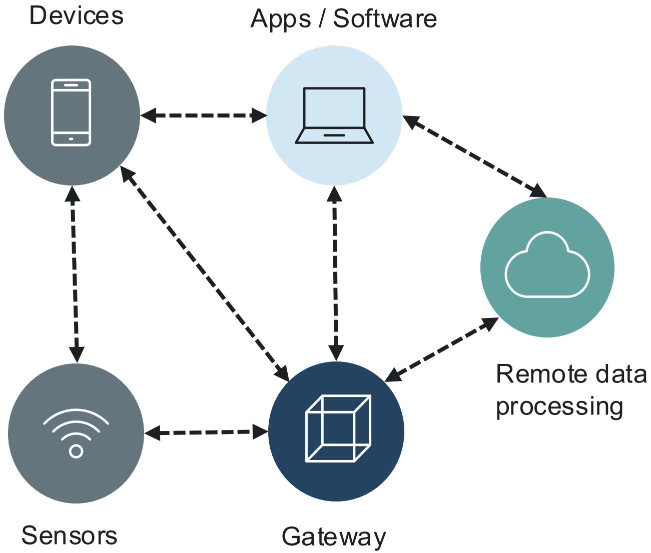
Source: CERT-EU | CISA KEV Apache Log4j2 CVE-2021-44228 | EUVD EUVD-2021-2544

03

Essential Requirements

Understanding of the essential requirements and relevant Vulnerability Handling 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

accessible action address advisory agreed applicable
apply available components contained
coordinated delay digital document
elements ensure facilitate
fixed format given helping identify
including
information issues machine-readable
manner manufacturers measures
mechanisms otherwise possibility potential
product providing
public relation relevant remediate reporting
risks security severity share software
taken technically updates users
vulnerabilities

□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

CRA’s Recitals mentioning vulnerability handling (1 of 4)

- (34) … **The vulnerability handling obligations** set out in this Regulation, which manufacturers have to comply with when placing a product with digital elements on the market and for the support period, **apply to products with digital elements in their entirety, including to all integrated components.** …

- (38) … Those essential cybersecurity requirements, including **vulnerability management handling requirements**, apply to **each individual product with digital elements when placed on the market,** irrespective of whether the product with digital elements is manufactured as an individual unit or in series. …

- (57) … To improve the transparency of vulnerability handling processes and to ensure that users are not required to install new functionality updates for the sole purpose of receiving the latest security updates, manufacturers should ensure, **where technically feasible**, that **new security updates are provided separately from functionality updates**.

CRA’s Recitals mentioning vulnerability handling (2 of 4)

❑(60) … **The support period for which the manufacturer ensures the effective handling of vulnerabilities should be no less than five years**, **unless the lifetime of the product with digital elements is less than five years**, in which case the manufacturer should ensure the vulnerability handling for that lifetime.

❑(61) **When products with digital elements reach the end of their support periods**, in order to ensure that vulnerabilities can be handled after the end of the support period, **manufacturers should consider releasing the source code of such products with digital elements either to other undertakings which commit to extending the provision of vulnerability handling services or to the public**. …

❑(63) Manufacturers should set up a **single point of contact** that enables users to communicate easily with them, including for the purpose of reporting on and receiving information about the vulnerabilities of the product with digital element**. They should make the single point of contact easily accessible for users and clearly indicate its availability**, keeping this information up to date. Where manufacturers choose to offer automated tools, e.g. chat boxes, they should also offer a phone number or other digital means of contact, such as an email address or a contact form. **The single point of contact should not rely exclusively on automated tools.**

CRA's Recitals mentioning vulnerability handling (3 of 4)

❑(76) Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities either directly to the manufacturer or indirectly, and where requested anonymously, via CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive (EU) 2022/2555. **Manufacturers' coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public.** Moreover, manufacturers should also consider publishing their security policies in machine-readable format. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, **manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts**. This refers to so-called '**bug bounty** programmes'.

CRA’s Recitals mentioning vulnerability handling (4 of 4)

❑(77) In order to facilitate **vulnerability analysis**, manufacturers should identify and document components contained in the products with digital elements, including by drawing up an **SBOM**. **An SBOM can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, in particular it helps manufacturers and users to track known newly emerged vulnerabilities and cybersecurity risks.** It is of particular importance that manufacturers ensure that their products with digital elements do not contain vulnerable components developed by third parties. Manufacturers should not be obliged to make the SBOM public.

CRA’s Article 13 Obligations of manufacturers

❑(6) **Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I.** Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.

- (7) The manufacturers **shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks**, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.

04

Vulnerability Handling

Prepare

PT3 Objectives

❑ Focus on creating a harmonized standard on vulnerability handling for products with digital elements aligned with the standardization request M/606 (horizontal scope)

❑ Covers the Essential Requirements of the CRA Annex I part II Vulnerability handling requirements (1) – (8)

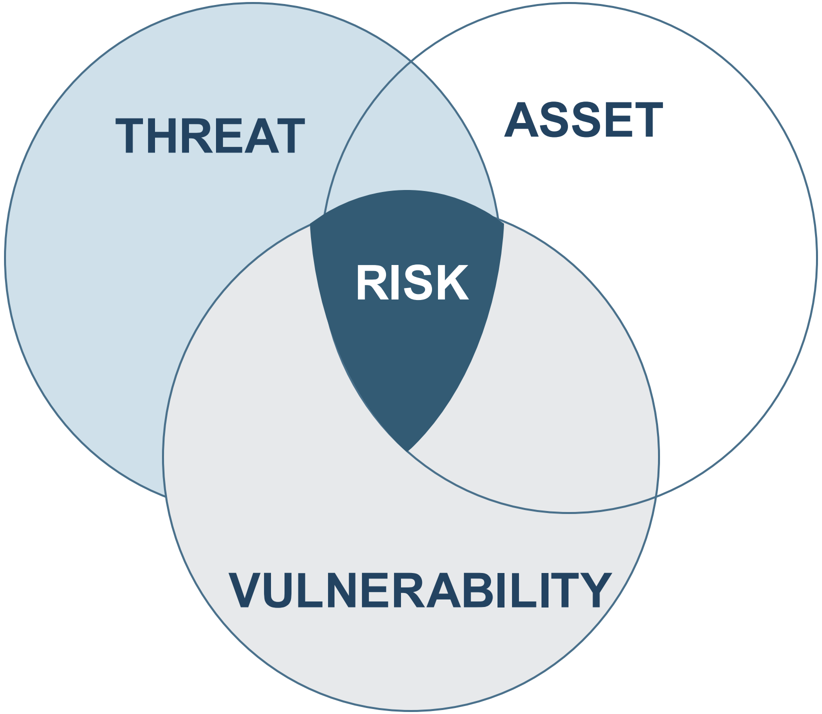
❑ This harmonized standard is expected to be published by **August 30, 2026**.

❑ Structure of the requirements in the standard will reflect the phases of the Coordinated Vulnerability disclosure (CVD) process to be in line with the ISO/IEC 29147:2018 and EN ISO/IEC 30111:2019

❑ The only horizontal standard of the three (PT1, PT2) that may be suited for citation to provide a presumption of conformity for Annex I, Part II.

❑ The expectation is that the vertical standards should be normatively referenced to the PT3 standard, with no or minimal changes.

Basic terminology



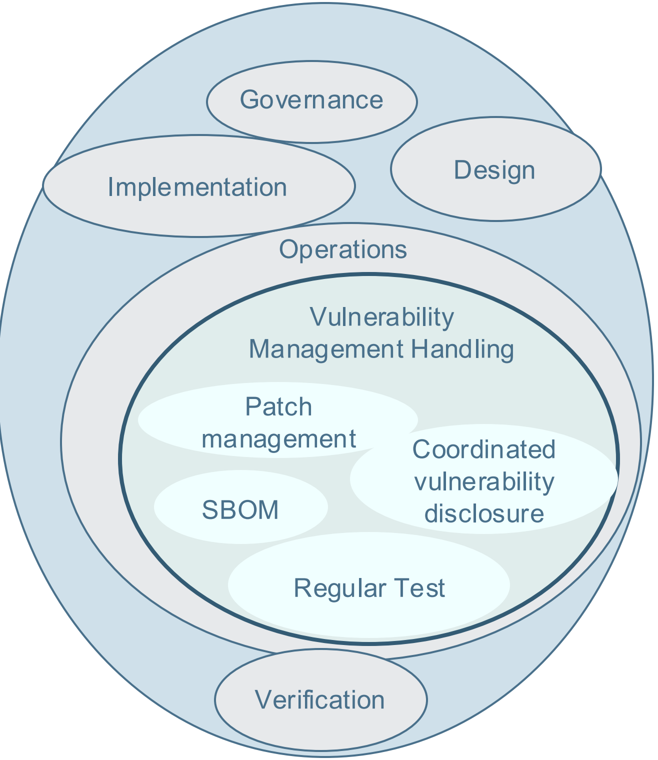
- ❑(37) **‘cybersecurity risk’** means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;
- ❑(40) **‘vulnerability’** means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat;.
- ❑(46) **‘cyber threat’** means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;
  - ❑‘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;
- ❑**‘asset’** physical entity or digital entity that has value to an individual, an organization, or a government

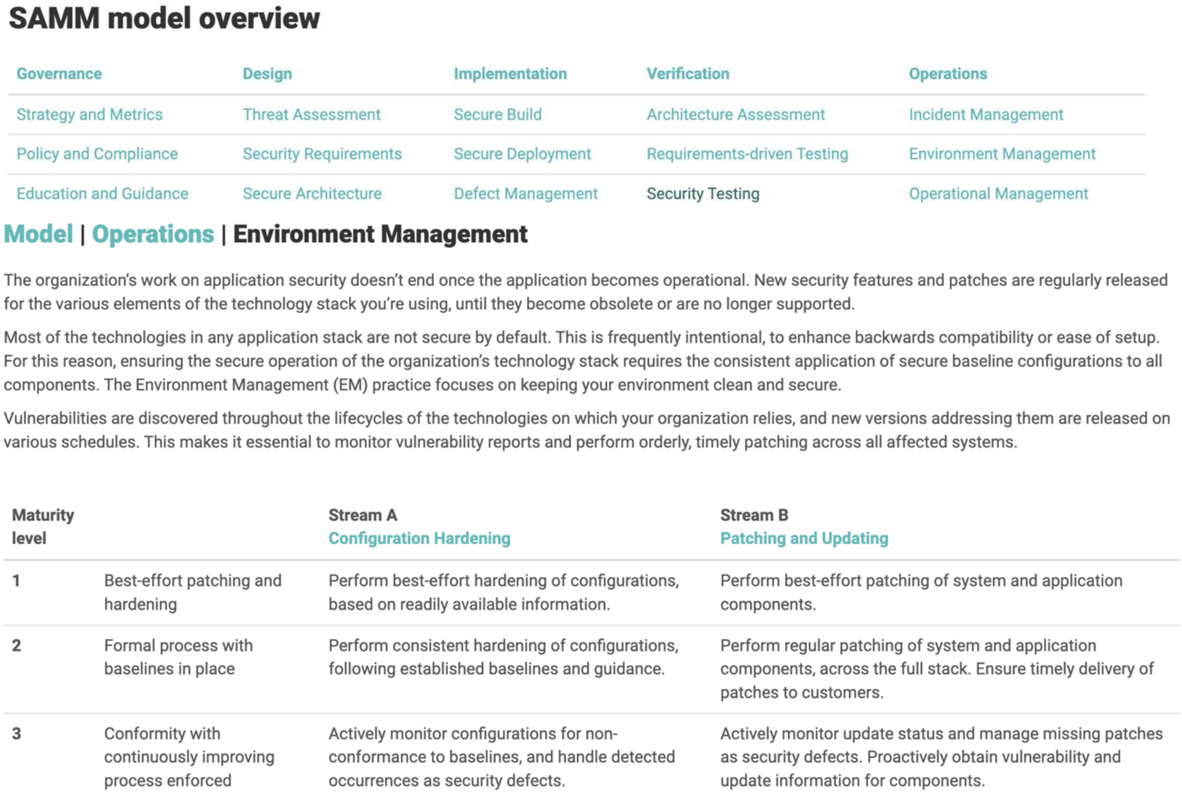
Vulnerability handling vs Incident Handling

- **Vulnerability handling** focuses on identifying and mitigating weaknesses in systems and applications before they can be exploited, essentially preventing incidents from happening.
- **Incident handling**, on the other hand, focuses on responding to and recovering from security incidents that have already occurred

Feature	Vulnerability handling	Incident Handling
Proactive/Reactive	**Proactive**	**Reactive**
Focus	Weaknesses	Security breaches
Goal	Prevent incidents	Recover from incidents
Primary Activity	Scanning, patching	Containment, eradication
Timeframe	Ongoing	Event-driven

Contestualization with a SDLC Maturity Model





SAMM model overview

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Secure Architecture	Defect Management	Security Testing	Operational Management

Model | Operations | Environment Management

The organization's work on application security doesn't end once the application becomes operational. New security features and patches are regularly released for the various elements of the technology stack you're using, until they become obsolete or are no longer supported.

Most of the technologies in any application stack are not secure by default. This is frequently intentional, to enhance backwards compatibility or ease of setup. For this reason, ensuring the secure operation of the organization's technology stack requires the consistent application of secure baseline configurations to all components. The Environment Management (EM) practice focuses on keeping your environment clean and secure.

Vulnerabilities are discovered throughout the lifecycles of the technologies on which your organization relies, and new versions addressing them are released on various schedules. This makes it essential to monitor vulnerability reports and perform orderly, timely patching across all affected systems.

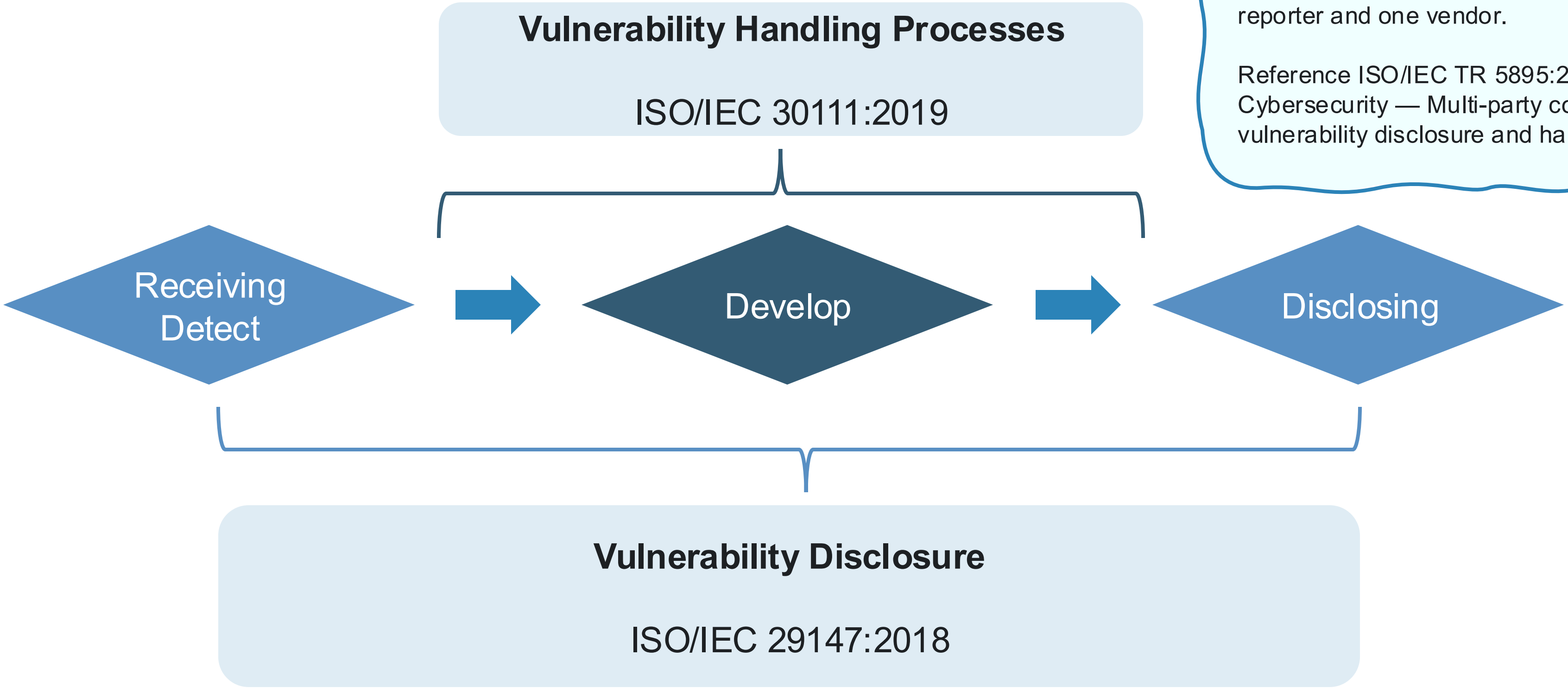
Maturity level		Stream A Configuration Hardening	Stream B Patching and Updating
1	Best-effort patching and hardening	Perform best-effort hardening of configurations, based on readily available information.	Perform best-effort patching of system and application components.
2	Formal process with baselines in place	Perform consistent hardening of configurations, following established baselines and guidance.	Perform regular patching of system and application components, across the full stack. Ensure timely delivery of patches to customers.
3	Conformity with continuously improving process enforced	Actively monitor configurations for non-conformance to baselines, and handle detected occurrences as security defects.	Actively monitor update status and manage missing patches as security defects. Proactively obtain vulnerability and update information for components.

Source: https://owaspsamm.org/model/operations/

Vulnerability lifecycle

Considerations: vulnerability disclosure and handling processes as described in ISO/IEC 29147 and ISO/IEC 30111 primarily focus on processes involving one reporter and one vendor.

Reference ISO/IEC TR 5895:2022(en) Cybersecurity — Multi-party coordinated vulnerability disclosure and handling



Vulnerability Handling Processes

ISO/IEC 30111:2019

Receiving Detect

Develop

Disclosing

Vulnerability Disclosure

ISO/IEC 29147:2018

Overview of the two standards

ISO/IEC 29147:2018

Description

- Focuses on actions visible to the outside
  - Policies to deal with vulnerabilities
  - How to receive vulnerabilities
  - How to publish information

Main sections

- Vulnerability disclosure policy
- Receiving Vulnerability Reports
- Publishing Vulnerability Advisories
- Coordination

ISO/IEC 30111:2019

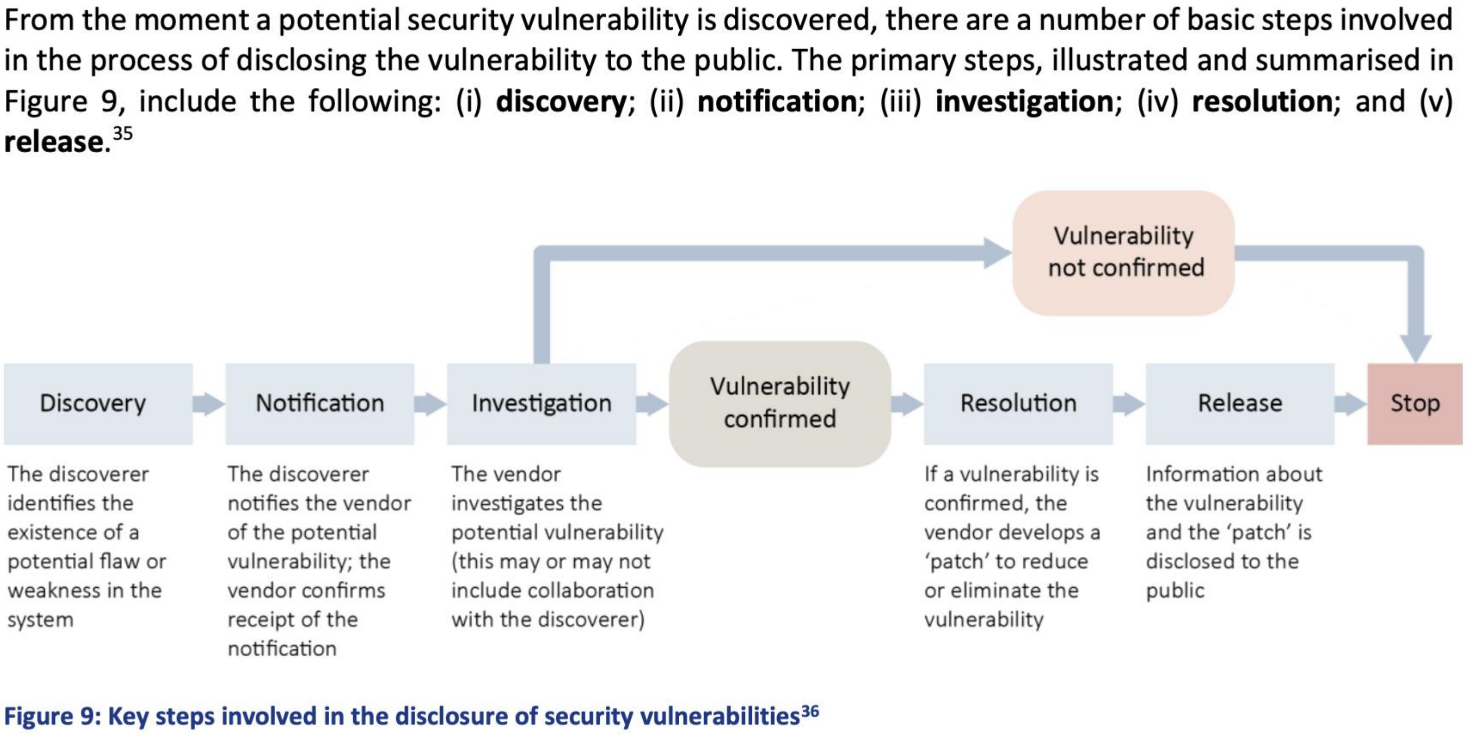
Description

- Focuses on handling procedures within the organization
  - Role and responsibilities
  - Definition of the phases on how to handle vulnerabilities
  - Process to monitor the vulnerabilities

Main sections

- Policies and organizational framework
- Vulnerability handling phase
  - General, Preparation, Receipt, Verification, Remediation, Development, Release, Post-release
- Process monitoring
- Confidentiality of vulnerability information
- Supply chain considerations

General steps involved in the disclosure of vulnerabilities



From the moment a potential security vulnerability is discovered, there are a number of basic steps involved in the process of disclosing the vulnerability to the public. The primary steps, illustrated and summarised in Figure 9, include the following: (i) **discovery**; (ii) **notification**; (iii) **investigation**; (iv) **resolution**; and (v) **release**.[35]

Discovery

The discoverer identifies the existence of a potential flaw or weakness in the system

Notification

The discoverer notifies the vendor of the potential vulnerability; the vendor confirms receipt of the notification

Investigation

The vendor investigates the potential vulnerability (this may or may not include collaboration with the discoverer)

Vulnerability confirmed

Vulnerability not confirmed

Resolution

If a vulnerability is confirmed, the vendor develops a 'patch' to reduce or eliminate the vulnerability

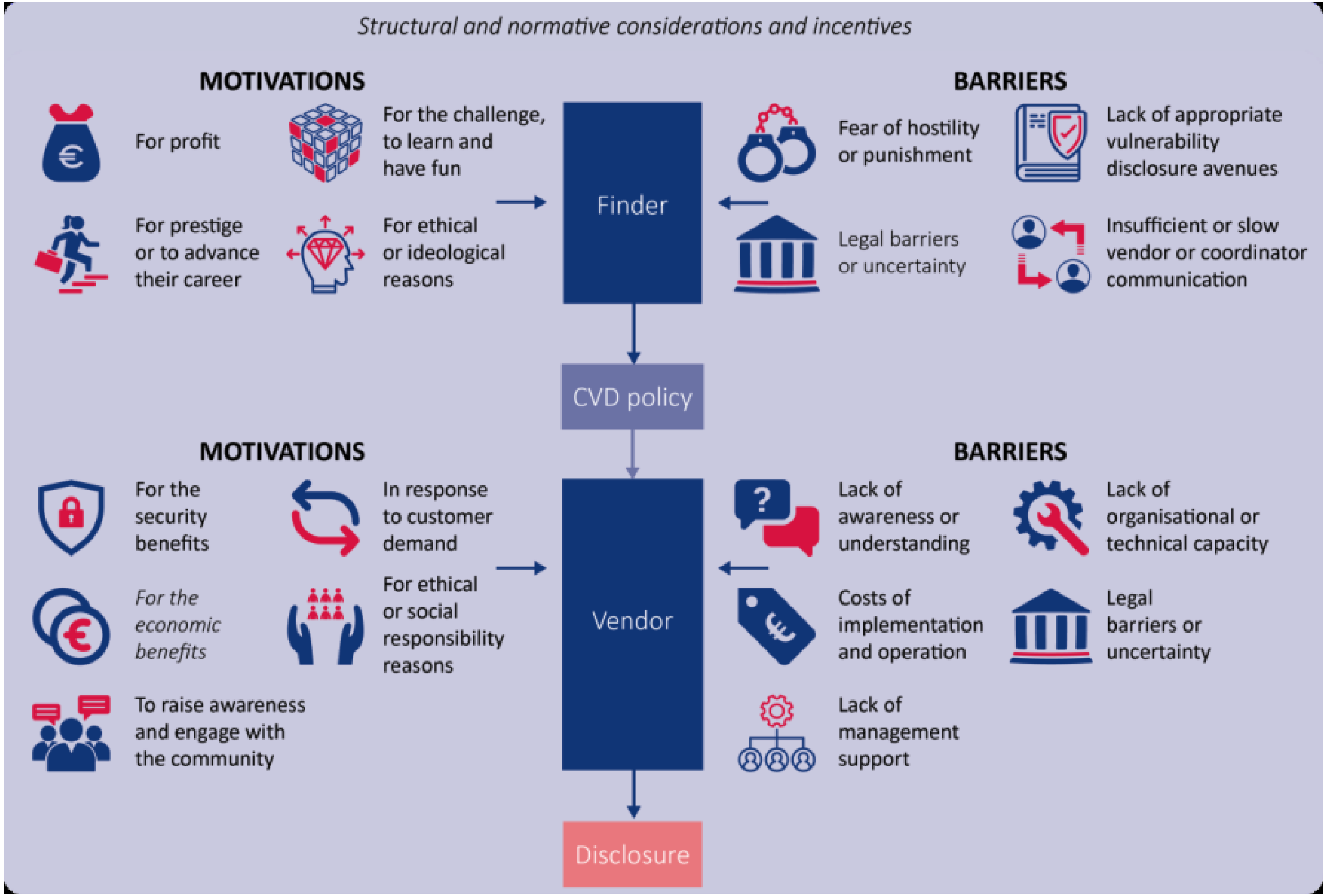
Release

Information about the vulnerability and the 'patch' is disclosed to the public

Stop

Figure 9: Key steps involved in the disclosure of security vulnerabilities[36]

Source: ENISA - Good Practice Guide on Vulnerability Disclosure - NOVEMBER 2015 / LINK



Structural and normative considerations and incentives

MOTIVATIONS

- For profit
- For the challenge, to learn and have fun
- For prestige or to advance their career
- For ethical or ideological reasons

Finder

BARRIERS

- Fear of hostility or punishment
- Lack of appropriate vulnerability disclosure avenues
- Legal barriers or uncertainty
- Insufficient or slow vendor or coordinator communication

CVD policy

MOTIVATIONS

- For the security benefits
- In response to customer demand
- *For the economic benefits*
- For ethical or social responsibility reasons
- To raise awareness and engage with the community

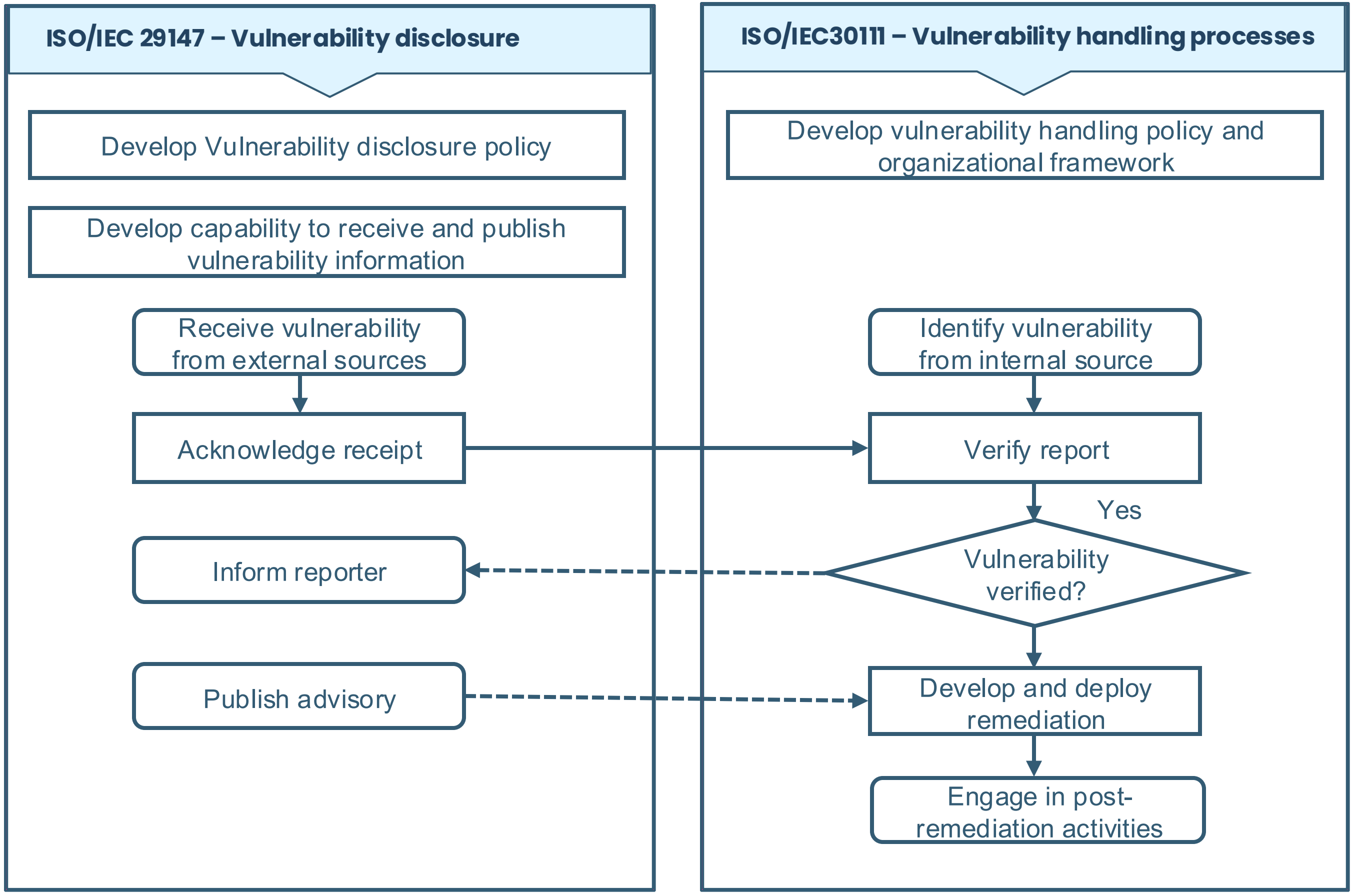
Vendor

BARRIERS

- Lack of awareness or understanding
- Lack of organisational or technical capacity
- Costs of implementation and operation
- Legal barriers or uncertainty
- Lack of management support

Disclosure

Source: ENISA - Economics of vulnerability disclosure (page 46), Publication date: December 14, 2018 (LINK)



ISO/IEC 29147 – Vulnerability disclosure

Develop Vulnerability disclosure policy

Develop capability to receive and publish vulnerability information

Receive vulnerability from external sources

Acknowledge receipt

Inform reporter

Publish advisory

ISO/IEC30111 – Vulnerability handling processes

Develop vulnerability handling policy and organizational framework

Identify vulnerability from internal source

Verify report

Yes

Vulnerability verified?

Develop and deploy remediation

Engage in post-remediation activities

Source: ISO/IEC 30111:2019 - Figure 1 — Relationship between ISO/IEC 29147 and ISO/IEC 30111 (page 2)

Draft Vulnerability Handling Structure

PREPARATION

- [PRE-1] Policy on coordinated vulnerability disclosure
  - EN ISO/IEC 29147:2020 Clause 9
- [PRE-2] Capability to receive reports
  - EN ISO/IEC 29147:2020 Clause 6.2.2
- [PRE-3] Contact Information
  - EN ISO/IEC 29147:2020 Clause 9.2.2
- [PRE-4] Secure communications
  - EN ISO/IEC 29147:2020 Clause 5.8.2
- [PRE-5] Product identification
- [PRE-6] Software components
- [PRE-7] Hardware components
- [PRE-8] Software Bill of Material (SBOM)

RECEIPT

- [RCP-1] Monitoring
- [RCP-2] Potentially impacted software components
- [RCP-3] Potentially impacted hardware components

VERIFICATION

- [VRF-1] Report verification
  - ISO 30111:2020 Clause 7.1.4 a. / 7.1.4 b. / 7.1.4 e.
- [VRF-2] Triage
  - ISO 30111:2020 Clause 7.1.4 a / 7.1.4 b
- [VRF-3] Vulnerability Risk Assessment
  - ISO 30111:2020 Clause 7.1.4 e
- [VRF-4] On-going communication
  - EN ISO/IEC 29147:2020 Clause 6.5
- [VRF-5] Coordinator involvement
  - EN ISO/IEC 29147:2020 Clause 5.5.5 / Clause 8.1
- [VRF-6] Operational security
  - EN ISO/IEC 29147:2020 Clause 6.7

REMEDIATION

- [RMD-1] Remediation Decision
  - ISO 30111:2020 Clause 7.15 a
- [RMD-2] Remediation Development
  - ISO 30111:2020 Clause 7.15 b
- [RMD-3] Remediation Test
  - ISO 30111:2020 Clause 7.15 c

RELEASE

- [RLS-1] Provisioning of Security Updates
  - ISO 30111:2020 Clause 7.1.6 a
- [RLS-2] Distribution of security update
- [RLS-3] Release Information
  - EN ISO/IEC 29147:2020 Clause 7.4 / 7.5 / 7.6 / 7.7

POST-RELEASE

- [PR-1] Post-release plan
  - ISO 30111:2020 Clause 7.1.7

Vulnir

Customer facing

Risk management

Internal Activities

PT3 - Vulnerability Handling – [PRE] Preparation

- **[PRE] Preparation**
- [RCP] Receipt
- [VRF] Verification
- [RMD] Remediation
- [RLS] Release
- [PRP] Post release

Goal:

- This phase involves establishing the appropriate **vulnerability disclosure policies** and procedures. The preparation phase also includes requirements such as formalizing the **Software Bill of Materials (SBOM)**, which supports the subsequent phases in identifying vulnerabilities and threats, as well as related potential automation, possibly using a machine-readable format.
- A manufacturer must take measures to facilitate the sharing of information about potential vulnerabilities in their product, including digital elements and third-party components, and provide a contact address for reporting vulnerabilities discovered in the product.

Requirements:

- [PRE-1] Policy on coordinated vulnerability disclosure(EN ISO/IEC 29147:2020 Clause 9)
- [PRE-2] Capability to receive reports (EN ISO/IEC 29147:2020 Clause 6.2.2)
- [PRE-3] Contact Information (EN ISO/IEC 29147:2020 Clause 9.2.2)
- [PRE-4] Secure communications (EN ISO/IEC 29147:2020 Clause 5.8.2)
- [PRE-5] Product identification
- [PRE-6] Software components
- [PRE-7] Hardware components
- [PRE-8] Software Bill of Material (SBOM)

Customer facing | Risk management | Internal Activities

PT3 - Vulnerability Handling – [RCP] Receipt

- [PRE] Preparation
- **[RCP] Receipt**
- [VRF] Verification
- [RMD] Remediation
- [RLS] Release
- [PRP] Post release

Goal:

- Become aware of vulnerabilities in the product, documentation, and processes from internal and external stakeholders. This includes, but is not limited to:
  - Reports received through CVD Internal testing
  - Bug reports from any source
  - Incidents reported internally or from the industry and researchers

Requirements:

- [RCP-1] Monitoring
- [RCP-2] Potentially impacted software components
- [RCP-3] Potentially impacted hardware components

Customer facing | Risk management | Internal Activities

PT3 - Vulnerability Handling – [VRF] VERIFICATION

- [PRE] Preparation
- [RCP] Receipt
- **[VRF] Verification**
- [RMD] Remediation
- [RLS] Release
- [PRP] Post release

Goal:

- Risk assess and prioritize vulnerabilities.
- This involves evaluating the risks, maintaining ongoing and secure communication between the parties involved

Requirements:

- [VRF-1] Report verification (ISO 30111:2020 Clause 7.1.4 a. / 7.1.4 b. / 7.1.4 e.)
- [VRF-2] Triage (ISO 30111:2020 Clause 7.1.4 a / 7.1.4 b)
- [VRF-3] Vulnerability Risk Assessment (ISO 30111:2020 Clause 7.1.4 e)
- [VRF-4] On-going communication (EN ISO/IEC 29147:2020 Clause 6.5)
- [VRF-5] Coordinator involvement (EN ISO/IEC 29147:2020 Clause 5.5.5 / 8.1)
- [VRF-6] Operational security (EN ISO/IEC 29147:2020 Clause 6.7)

Customer facing | Risk management | Internal Activities

PT3 - Vulnerability Handling – [RMD] REMEDIATION

- [PRE] Preparation
- [RCP] Receipt
- [VRF] Verification
- **[RMD] Remediation**
- [RLS] Release
- [PRP] Post release

Goal:

- Once a vulnerability has been verified and a decision made to address it, remediation may be required, typically involving mitigation controls in the form of a tested patch or security update.

Requirements:

- [RMD-1] Remediation Decision (ISO 30111:2020 Clause 7.1.5 a)
- [RMD-2] Remediation Development (ISO 30111:2020 Clause 7.1.5 b)
- [RMD-3] Remediation Test (ISO 30111:2020 Clause 7.1.5 c)

Customer facing | Risk management | Internal Activities

PT3 - Vulnerability Handling – [RLS] RELEASE

- [PRE] Preparation
- [RCP] Receipt
- [VRF] Verification
- [RMD] Remediation
- **[RLS] Release**
- [PRP] Post release

Goal:

- This phase includes deploying remediation, describing associated changes, and sharing information with relevant stakeholders.

Requirements:

- [RLS-1] Provisioning of Security Updates (ISO 30111:2020 Clause 7.1.6 a)
- [RLS-2] Distribute of security update
- [RLS-3] Release Information (EN ISO/IEC 29147:2020 Clause 7.4 / 7.5 / 7.6 / 7.7)

Customer facing | Risk management | Internal Activities

PT3 - Vulnerability Handling – [PRP] POST RELEASE

- [PRE] Preparation
- [RCP] Receipt
- [VRF] Verification
- [RMD] Remediation
- [RLS] Release
- **[PRP] Post release**

Goal:

- This phase includes monitoring of the released update. Lessons learned and reflections during the post-release may even lead to changes and improvements in the development process.

Requirements:

- [PR-1] Post release plan (ISO 30111:2020 Clause 7.1.7)

Customer facing | Risk management | Internal Activities

05

Vulnerability Handling: Deep Dive

Exploring each section providing status and challenges

PT3 - Vulnerability Handling – [PRE] Preparation

[PRE] Preparation

[RCP] Receipt

[VRF] Verification

[RMD] Remediation

[RLS] Release

[PRP] Post release

Goal:

- This phase involves establishing the appropriate **vulnerability disclosure policies** and procedures. The preparation phase also includes requirements such as formalizing the **Software Bill of Materials (SBOM)**, which supports the subsequent phases in identifying vulnerabilities and threats, as well as related potential automation, possibly using a machine-readable format.
- A manufacturer must take measures to facilitate the sharing of information about potential vulnerabilities in their product, including digital elements and third-party components, and provide a contact address for reporting vulnerabilities discovered in the product.

Requirements:

- [PRE-1] Policy on coordinated vulnerability disclosure(EN ISO/IEC 29147:2020 Clause 9)
- [PRE-2] Capability to receive reports (EN ISO/IEC 29147:2020 Clause 6.2.2)
- [PRE-3] Contact Information (EN ISO/IEC 29147:2020 Clause 9.2.2)
- [PRE-4] Secure communications (EN ISO/IEC 29147:2020 Clause 5.8.2)
- [PRE-5] Product identification
- [PRE-6] Software components
- [PRE-7] Hardware components
- [PRE-8] Software Bill of Material (SBOM)

🟨 Customer facing 🟦 Risk management 🟩 Internal Activities

5.1.2 [PRE-1] Policy on coordinated vulnerability disclosure

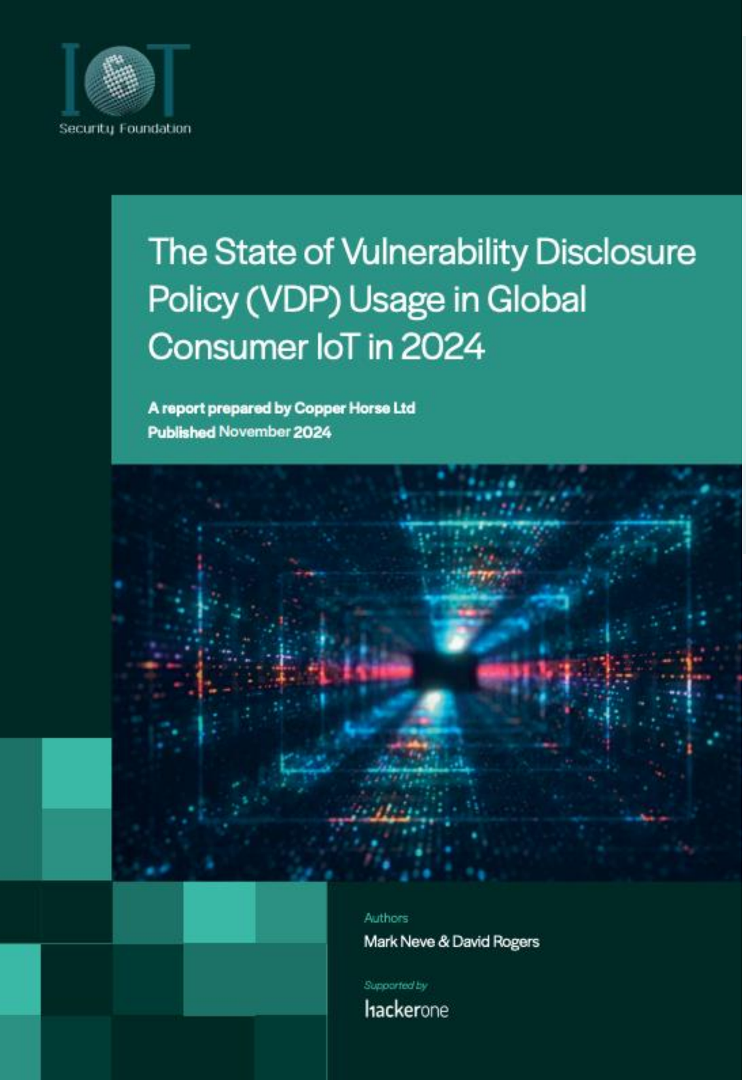
PREPARATION

- Essential requirement:
  - **(5) put in place and enforce a policy on coordinated vulnerability disclosure;**

- Essential requirement:
  - **5.1.2 [PRE-1]**

- **Requirement**:
  - Essentially, we are requiring a CVD that is in line with EN ISO/IEC 29147:2020 Clause 9
- **Input**:
  - Organisational policies
- **Output**:
  - CVD
- **Assessment**
  - CVD and evidence that the process is followed

- **Notes on the state of the art** (ISO/IEC 29147):
  - ETSI TR 103 838 V1.1.1 (2022-01) - Guide to Coordinated Vulnerability Disclosure
  - EN 303 645 - V3.1.3 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements (Provision 5.2-1)
- **Examples**:
  - https://www.etsi.org/standards/coordinated-vulnerability-disclosure
  - https://www.rapid7.com/security/disclosure/
  - https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html
  - https://security.openstack.org/vmt-process.html



IoT Security Foundation

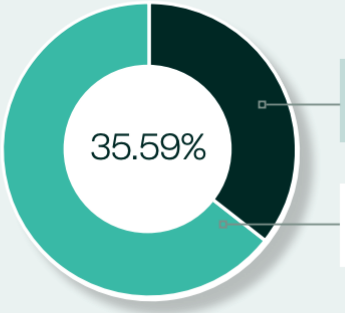
The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2024

A report prepared by Copper Horse Ltd
Published November **2024**

Authors
Mark Neve & David Rogers

Supported by
hackerone

The Headline Figure

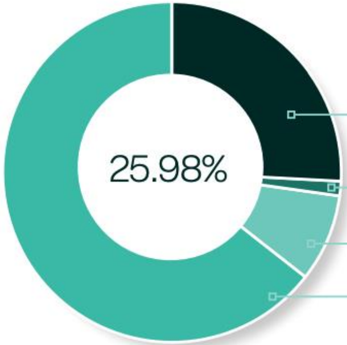


35.59% of the companies had a way for security researchers to contact them

64.41% of the companies didn't have a way for security researchers to contact them

Figure 2

Figure 5



25.98%
Coordinated Vulnerability Disclosure (CVD)

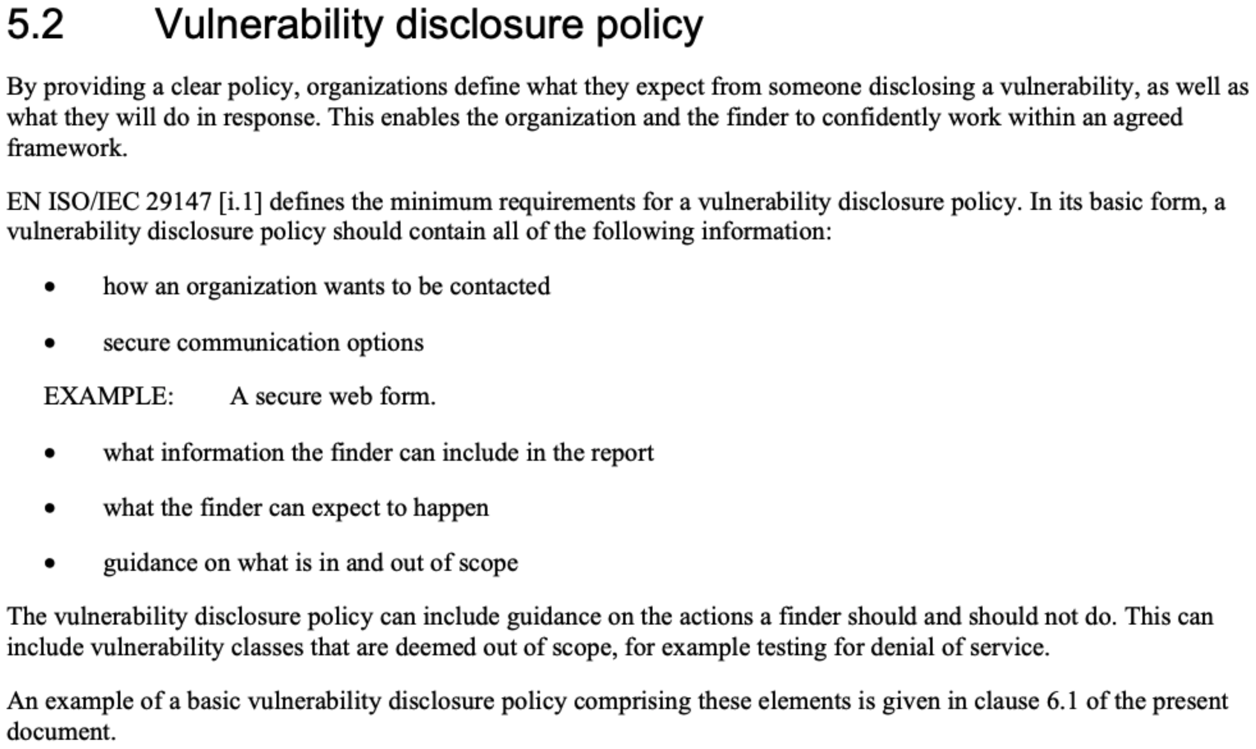
1.31%
Non-disclosure Policy

8.30%
Vulnerability Disclosure Policy (VDP), but type not declared

64.41%
No Vulnerability Disclosure Policy (VDP)

Source: IoT Security Foundation - The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2024, Publication date: November 2024 (LINK)

ETSI TR 103 838 V1.1.1 (2022-01) - Vulnerability Disclosure policy



5.2 Vulnerability disclosure policy

By providing a clear policy, organizations define what they expect from someone disclosing a vulnerability, as well as what they will do in response. This enables the organization and the finder to confidently work within an agreed framework.

EN ISO/IEC 29147 [i.1] defines the minimum requirements for a vulnerability disclosure policy. In its basic form, a vulnerability disclosure policy should contain all of the following information:

- how an organization wants to be contacted
- secure communication options

EXAMPLE: A secure web form.

- what information the finder can include in the report
- what the finder can expect to happen
- guidance on what is in and out of scope

The vulnerability disclosure policy can include guidance on the actions a finder should and should not do. This can include vulnerability classes that are deemed out of scope, for example testing for denial of service.

An example of a basic vulnerability disclosure policy comprising these elements is given in clause 6.1 of the present document.

Source: ETSI TR 103 838 V1.1.1 (2022-01) - Cyber Security; Guide to Coordinated Vulnerability Disclosure (LINK)

5.1.3 [PRE-2] Capability to receive reports

PREPARATION

- Essential requirement:
  - (6) **take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product**, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

- Essential requirement:
  - Covered by
    - **5.1.3 [PRE-2]**
    - 5.1.4 [PRE-3]
    - 5.1.5 [PRE-4]

- **Requirement**:
  - Essentially, the capability to receive a report based on EN ISO/IEC 29147:2020 Clause 6.2.2
- **Input**:
  - Set as none, but should be part of the CVD Policy
- **Output**:
  - One or multiple reporting mechanisms present
- **Assessment**
  - Public reporting mechanism form, and that works as expected
  - Evidence of reports received with tracking number

- **Notes on the state of the art** (ISO/IEC 29147):
  - UK PSTI (LINK)
    - Information on how to report security issues
      - 3 (a) how a person may access the mechanism for the manufacturer to receive reports described in paragraph 6.2.2 of ISO/IEC 29147;
- **Examples**:
  - https://www.etsi.org/standards/coordinated-vulnerability-disclosure
  - https://www.rapid7.com/security/disclosure/
  - https://www.nestle.com/ask-nestle/our-company/answers/vulnerability-disclosure-program

5.1.4 [PRE-3] Contact Information

PREPARATION

- Essential requirement:
  - (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including **by providing a contact address for the reporting of the vulnerabilities discovered** in the product with digital elements;

- Essential requirement:
  - Covered by
    - 5.1.3 [PRE-2]
    - **5.1.4 [PRE-3]**
    - 5.1.5 [PRE-4]

- **Requirement**:
  - Essentially, what is specified already in EN ISO/IEC 29147:2020 Clause 9.2.2 and included as an element in the 5.1.2 [PRE-1]
- **Input**:
  - 5.1.3 [PRE-2]
- **Output**:
  - One or multiple contact information
- **Assessment**
  - Contact information present and working

- **Notes on the state of the art** (ISO/IEC 29147):
  - UK PSTI (LINK)
    - Information on how to report security issues
      - 2 (a) at least one point of contact to allow a person (“P”) to report to the manufacturer security issues relating to the categories listed in sub-paragraph (1) for any of the manufacturer’s relevant connectable products for which they have an obligation under section 8 (duty to comply with security requirements);
  - EN 303 645 - V3.1.3 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements (Provision 5.2-1)
- **Examples**:
  - https://www.etsi.org/standards/coordinated-vulnerability-disclosure
    - Helpdesk@etsi.org

5.1.5 [PRE-4] Secure communication

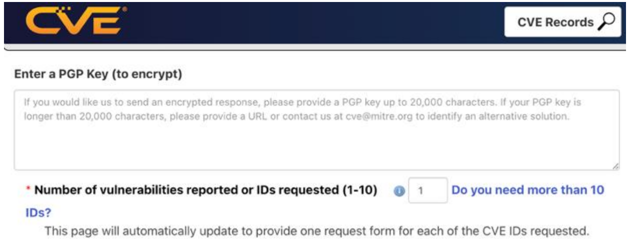
PREPARATION

- Essential requirement:
  - (6) **take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product,** including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

- Essential requirement:
  - Covered by
    - 5.1.3 [PRE-2]
    - 5.1.4 [PRE-3]
    - **5.1.5 [PRE-4]**

- **Requirement**:
  - Not explicitly mentioned in the essential requirement, but the report should be communicated in a secure manner
  - Essentially, what is specified already in EN ISO/IEC 29147:2020 Clause 5.8.2 and included already as an element in the 5.1.2 [PRE-1] and provided in EN ISO/IEC 29147:2020 Clause 9.3.3
- **Input**:
  - 5.1.3 [PRE-2]
- **Output**:
  - Where feasible, a practical and secure communication method was implemented (eg. secure web form)
- **Assessment**
  - Evaluate if there is a secure channel in place (HTTPS / OpenPGP)

- **Notes on the state of the art** (ISO/IEC 29147):
- **Examples**:
  - https://security.openstack.org/vmt-process.html
  - https://cveform.mitre.org/



Enter a PGP Key (to encrypt)

If you would like us to send an encrypted response, please provide a PGP key up to 20,000 characters. If your PGP key is longer than 20,000 characters, please provide a URL or contact us at cve@mitre.org to identify an alternative solution.

* Number of vulnerabilities reported or IDs requested (1-10) 1 Do you need more than 10 IDs?

This page will automatically update to provide one request form for each of the CVE IDs requested.

5.1.6 [PRE-5] Product identification

PREPARATION

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

- Essential requirement:
  - Covered by
    - **5.1.6 [PRE-5]**
    - 5.5.4 [RLS-3]

- **Requirement**:
  - Essentially, provision to have unambiguously identify the device and include at least the Manufacturer, Product name, Product version
- **Input**:
  - None
- **Output**:
  - Product identification
- **Assessment**
  - Evidence of the existence of product identification information

- **Notes on the state of the art** :
  - Article 13 - Obligations of manufacturers
    - 15. Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, that that information is provided on their packaging or in a document accompanying the product with digital elements.
  - ANNEX II - INFORMATION AND INSTRUCTIONS TO THE USER
    - 3. name and type and any additional information enabling the unique identification of the product with digital elements;

5.1.7 [PRE-6] Software components

PREPARATION

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

- Essential requirement:
  - Covered by
    - **5.1.7 [PRE-6]**
    - 5.1.8 [PRE-7]
    - 5.1.9 [PRE-8]

- Covered by
  - 5.2.2 [RCP-1]
  - 5.2.3 [RCP-2]
  - 5.2.4 [RCP-3]

- **Requirement**:
  - Process to support the listing of all the software components that are part of the product, including in-house developed, third party, or open source. The information is similar to what has been asked for PRE-5 (manufacturer, component name, component version)
- **Input**:
  - None
- **Output**:
  - Software component list
- **Assessment**
  - Evidence of the existence of the list of software components and validation

- **Notes on the state of the art** :
  - CISA Guidance: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), October 2024 (LINK)
  - ISO/IEC 27036-3:2023 - Cybersecurity — Supplier relationships Part 3: Guidelines for hardware, software, and services supply chain security (Edition 2, 2023)
  - BSI - Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0 (PDF) (LINK)
  - Various format:
    - SPDX, the Software Package Data Exchange
    - CycloneDX Bill of Materials Specification (ECMA-424) (LINK)

5.1.8 [PRE-7] Hardware components

PREPARATION

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

- Essential requirement:
  - Covered by
    - 5.1.7 [PRE-6]
    - **5.1.8 [PRE-7]**
    - 5.1.9 [PRE-8]

- Covered by
  - 5.2.2 [RCP-1]
  - 5.2.3 [RCP-2]
  - 5.2.4 [RCP-3]

- **Requirement**:
  - Process to support the listing of all the hardware components that are part of the product, including in-house developed, third party, or open source. The information is similar to what has been asked for PRE-5 (manufacturer, component name, component version)
- **Input**:
  - None
- **Output**:
  - hardware component list
- **Assessment**
  - Evidence of the existence of the list of hardware components and validation

- **Notes on the state of the art** :
  - CISA Guidance: Hardware Bill of Materials Framework (HBOM) for Supply Chain Risk Management, September 2023 (LINK)
  - ISO/IEC 27036-3:2023 - Cybersecurity — Supplier relationships Part 3: Guidelines for hardware, software, and services supply chain security (Edition 2, 2023)
  - BSI - Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products - Part 2: Software Bill of Materials (SBOM) Version 2.0.0 (PDF) (LINK)
  - Various format:
    - SPDX, the Software Package Data Exchange
    - CycloneDX Bill of Materials Specification (ECMA-424) (LINK)

5.1.9 [PRE-8] Software Bill of Material (SBOM)

PREPARATION

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

- Essential requirement:
  - Covered by
    - 5.1.7 [PRE-6]
    - 5.1.8 [PRE-7]
    - **5.1.9 [PRE-8]**
  - Covered by
    - 5.2.2 [RCP-1]
    - 5.2.3 [RCP-2]
    - 5.2.4 [RCP-3]

- **Requirement**:
  - Definition of SBOM with the Manufacturer name, component name, component version
  - Include the relationship of components provided by the supplier (at least the first level of suppliers)
- **Input**:
  - Output [PRE-6] Software components
- **Output**:
  - SBOM
- **Assessment**
  - Evidence of SBOM in a structured machine-readable format

- **Notes on the state of the art** :
  - CISA Guidance: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM), October 2024 (LINK)
  - ISO/IEC 27036-3:2023 - Cybersecurity — Supplier relationships Part 3: Guidelines for hardware, software, and services supply chain security (Edition 2, 2023)
  - National Cyber Security Center (Netherlands): Software Bill of Materials Starter Guide, July 2024 (LINK)
  - SAFECode Managing Security Risks Inherent in the Use of Thirdparty Components, May 2017 (LINK)
  - Various formats:
    - SPDX, the Software Package Data Exchange
    - CycloneDX Bill of Materials Specification (ECMA-424) (LINK)

[PRE] Open discussion / Considerations

- ❑ We focused only on ISO/IEC 29147 Clause 9, which **is external vulnerability handling.** We should also consider making it normative ISO/IEC 30111:2019, Section 6.3, Vulnerability Handling Policy Development, which outlines an **internal vulnerability handling policy.** Does it make sense to make it normative only for the external vulnerability handling policy?

- ❑ Should we extend the vulnerability handling to capture the **multi-party nature of a coordinated vulnerability disclosure and handling**? Should we consider ISO/IEC TR 5895:2022(en) Cybersecurity — Multi-party coordinated vulnerability disclosure and handling?

- ❑ Should we require an explicit declaration for the **Hardware Bill of Materials**?

- ❑ How specific can we be in defining the **minimum elements required for the SBOM**? (eg, reference ISO/IEC 27036-3 - Guidelines for information and communication technology supply chain security)

- ❑ Can we make it normative as per **ISO/IEC 29147:2018, 5.4.6 and 6.4** to mandate manufacturers to define more formally the supply chain relationships beyond the SBOM? If yes, what would be the minimal elements? Can we use ISO/IEC 27036-3 as a normative reference?

- ❑ The CRA requirement is reciting "**covering at the very least the top-level dependencies of the products** ." Would that be enough?
  - ❑ Can we state in the requirement as in CISA publication (September 3, 2024 - LINK): **Minimum Expected** - SBOMs are expected to identify all static, direct Dependencies of the root or primary Component.
  - ❑ Another example of explicit elements: NTIA - The Minimum Elements For a Software Bill of Materials (SBOM) (July 12 2021, LINK)

- ❑ Interesting, the TR-03183 Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products on the appropriate level of details from SBOM (September, 20 2024, LINK)

5.1 [PRE] Preparation

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

PT3 - Vulnerability Handling – [RCP] Receipt

- [PRE] Preparation
- **[RCP] Receipt**
- [VRF] Verification
- [RMD] Remediation
- [RLS] Release
- [PRP] Post release

Goal:

- Become aware of vulnerabilities in the product, documentation, and processes from internal and external stakeholders. This includes, but is not limited to:
  - Reports received through CVD Internal testing
  - Bug reports from any source
  - Incidents reported internally or from the industry and researchers

Requirements:

- [RCP-1] Monitoring
- [RCP-2] Potentially impacted software components
- [RCP-3] Potentially impacted hardware components

Customer facing | Risk management | Internal Activities

5.2.2 [RCP-1] Monitoring

RECEIPT

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

- Essential requirement:
  - Covered by
    - 5.1.7 [PRE-6]
    - 5.1.8 [PRE-7]
    - 5.1.9 [PRE-8]
  - Covered by
    - **5.2.2 [RCP-1]**
    - 5.2.3 [RCP-2]
    - 5.2.4 [RCP-3]

- **Requirement**:
  - Not explicitly mentioned :
    - External monitoring: EN ISO/IEC 29147:2020 Clause 6.2.3 Monitoring
    - Internal monitoring: EN ISO/IEC 30111:2020 Clause 7.1.3 Receipt
  - Monitoring of internal and external sources shall be conducted to collect information about vulnerabilities
- **Input**:
  - Internal/external list of sources monitored
- **Output**:
  - Vulnerability reports
- **Assessment**
  - Verify the active process of feeding from sources / verification of vulnerability reports

- **Notes on the state of the art** (ISO/IEC 29147, ISO/IEC 30111):
  - **Already integrated**
    - Internal
      - [RCP-2] / [RCP-3]
    - External
      - [PRE-2]
  - **Not explicitly integrated yet**
    - Internal
      - Vulnerability Assessment / Monitoring / Tooling
      - Penetration Test
      - Threat Intelligence
    - External
      - The European Vulnerability Database (EUVD)
    - **Potential reference ISO/IEC 30111:2019 6.5.3 PSIRT responsibilities**

5.2.3 [RCP-2] Potentially impacted software components

RECEIPT

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

- Essential requirement:
  - Covered by
    - 5.1.7 [PRE-6]
    - 5.1.8 [PRE-7]
    - 5.1.9 [PRE-8]
  - Covered by
    - 5.2.2 [RCP-1]
    - **5.2.3 [RCP-2]**
    - 5.2.4 [RCP-3]

- **Requirement**:
  - Monitor that the components in the SBOM don't contain known vulnerabilities from internal and external sources [ref **RCP-1**]
  - Not explicitly mentioned / GAP :
    - Hardware, since the hardware list is not an input for the SBOM in our definition / but covered RCP-3
- **Input**:
  - [5.1.9] Software Bill of Materials output
- **Output**:
  - Vulnerabilities identified
- **Assessment**
  - Evidence of the identified vulnerabilities in software components

- **Notes on the state of the art**:
  - Techniques / Tools
    - Software Composition Analysis tool
    - Vulnerability Scan
    - Static code analysis
    - Firmware analysis

5.2.3 [RCP-3] Potentially impacted hardware components

RECEIPT

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

- Essential requirement:
  - Covered by
    - 5.1.7 [PRE-6]
    - 5.1.8 [PRE-7]
    - 5.1.9 [PRE-8]

- Covered by
  - 5.2.2 [RCP-1]
  - **5.2.3 [RCP-2]**
  - 5.2.4 [RCP-3]

- **Requirement**:
  - Monitor that the components in the **hardware** component list don't contain known vulnerabilities from internal and external sources [ref **RCP-1**]
- **Input**:
  - [5.1.8] Hardware components output
- **Output**:
  - Vulnerabilities identified
- **Assessment**
  - Evidence of the identified vulnerabilities in **hardware** components

- **Notes on the state of the art** :
  - Note to be discussed:
    - Could we make a stronger requirement for introducing HBOM?

[RCP] Open discussion / Considerations

❑The monitoring activities can be more specific, e.g., monitoring for EOL, Changes in the risk profile, and so on (ref. SAFECode: Managing Security Risks Inherent in the Use of Third-party Components, page 15 - LINK).

❑Should we include only the bare minimum, such as monitoring the European Vulnerability Database (EUVD)?

❑How can the regular testing activities be integrated? What are the activities that can be considered a bare minimum, eg, Vulnerability Assessment activities?

❑Would it make sense to introduce a normative reference on having an HBOM?

❑Which practices should be integrated for the supply chain cybersecurity practices (ref. ENISA Good Practices for Supply Chain Cybersecurity, June 2023, LINK)

5.2 [RCP] RECEIPT

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

PT3 - Vulnerability Handling – [VRF] VERIFICATION

- [PRE] Preparation
- [RCP] Receipt
- **[VRF] Verification**
- [RMD] Remediation
- [RLS] Release
- [PRP] Post release

Goal:

- Risk assess and prioritize vulnerabilities.
- This involves evaluating the risks, maintaining ongoing and secure communication between the parties involved

Requirements:

- [VRF-1] Report verification (ISO 30111:2020 Clause 7.1.4 a. / 7.1.4 b. / 7.1.4 e.)
- [VRF-2] Triage (ISO 30111:2020 Clause 7.1.4 a / 7.1.4 b)
- [VRF-3] Vulnerability Risk Assessment (ISO 30111:2020 Clause 7.1.4 e)
- [VRF-4] On-going communication (EN ISO/IEC 29147:2020 Clause 6.5)
- [VRF-5] Coordinator involvement (EN ISO/IEC 29147:2020 Clause 5.5.5 / 8.1)
- [VRF-6] Operational security (EN ISO/IEC 29147:2020 Clause 6.7)

Customer facing | Risk management | Internal Activities

5.3.2 [VRF-1] Report verification

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - **5.3.2 [VRF-1]**
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]
  - Covered by
    - 5.3.6 [VRF-5]
    - 5.3.7 [VRF-6]
    - 5.4.2 [RMD-1]
    - 5.4.3 [RMD-2]

- **Requirement**:
  - Essentially, the capability to verify a report based on EN ISO/IEC 30111:2020 Clause 7.1.4 (a) for the initial investigation and Clause 7.1.4 (b) for the possible exit process and Clause 7.1.4 (e) for the prioritization
- **Input**:
  - Internal/external list of sources monitored
- **Output**:
  - Uniquely identifiable, tracked and enhanced vulnerability report
- **Assessment**
  - Evidence on validation and investigation decision and all the potential exit process defined in 7.1.4 (b)

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.4 (a) Initial investigation
    - Clause 7.1.4 (b) possible process exit
    - Clause 7.1.4 (e) prioritization

Note: It could be more appropriate to reference ISO/IEC 29147:2018, Section 6.3 Initial Assessment

5.3.3 [VRF-2] Triage

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - **5.3.3 [VRF-2]**
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]
    - 5.3.6 [VRF-5]
    - 5.3.7 [VRF-6]
    - 5.4.2 [RMD-1]
    - 5.4.3 [RMD-2]

- **Requirement**:
  - Building on [VRF-1] Report verification
  - Expedite known exploitable vulnerabilities
  - Inform the reporter if a reported vulnerability is not considered valid
- **Input**:
  - Verified report as per [VRF-1]
  - Security architecture and design
- **Output**:
  - Uniquely identifiable, tracked vulnerability report with an outcome of the investigation
- **Assessment**
  - Evidence initial assessment
  - Documented resolution if vulnerability is not applicable or duplicate exists
  - Evidence of speeding up the analysis of known exploited vulnerability

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.4 (a) Initial investigation
    - Clause 7.1.4 (b) possible process exit

Note: Potential duplication with [VRF-1]

5.3.4 [VRF-3] Vulnerability Risk Assessment

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - **5.3.4 [VRF-3]**
    - 5.3.5 [VRF-4]

  - Covered by
    - 5.3.6 [VRF-5]
    - 5.3.7 [VRF-6]
    - 5.4.2 [RMD-1]
    - 5.4.3 [RMD-2]

- **Requirement**:
  - Building on EN ISO/IEC 30111:2020 Clause 7.1.4 (e) Prioritization
  - Risk assessed according to PT1
- **Input**:
  - Initial assessment report as per [VRF-1]
  - Triage report as per [VRF-2]
- **Output**:
  - Tracked and prioritized list of vulnerabilities with their assessed risks
- **Assessment**
  - A prioritized list of vulnerabilities with their assessed risks is available.

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.4 (e) Prioritization

Note:
- Need improvement and better contextualization of the risks assessment
- Better interplay and contextualization with PT1

5.3.5 [VRF-4] On-going communication

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - **5.3.5 [VRF-4]**
  - Covered by
    - 5.3.6 [VRF-5]
    - 5.3.7 [VRF-6]
    - 5.4.2 [RMD-1]
    - 5.4.3 [RMD-2]

- **Requirement**:
  - Ongoing communication with the reporter according to EN ISO/IEC 29147:2020 Clause 6.5
- **Input**:
  - Verified report as per [VRF-1]
  - Triaged report as per [VRF-2]
  - Risk Assessed vulnerabilities as per [VRF-3]
- **Output**:
  - Communication with the stakeholders
- **Assessment**
  - Evidence exists that communication with stakeholders is performed

Note: Is it reasonable to ask for a ticketing system?

- **Notes on the state of the art** :
  - EN ISO/IEC 29147:2020
    - Clause 6.5 on-going communication
- **Examples**:
  - Example of a vulnerability with maintained communication until the patch is released
    - [ZSL-2019-5542] [ZSL-2025-5923]
  - Example of no response [ZSL-2025-5931] [ZSL-2023-5769]

Macedonian Information Security Research & Development Laboratory

- Website: https://www.zeroscience.mk
- Credits: Gjoko Krstic - gjoko@zeroscience.mk

Vulnir

5.3.6 [VRF-5] Coordinator involvement

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

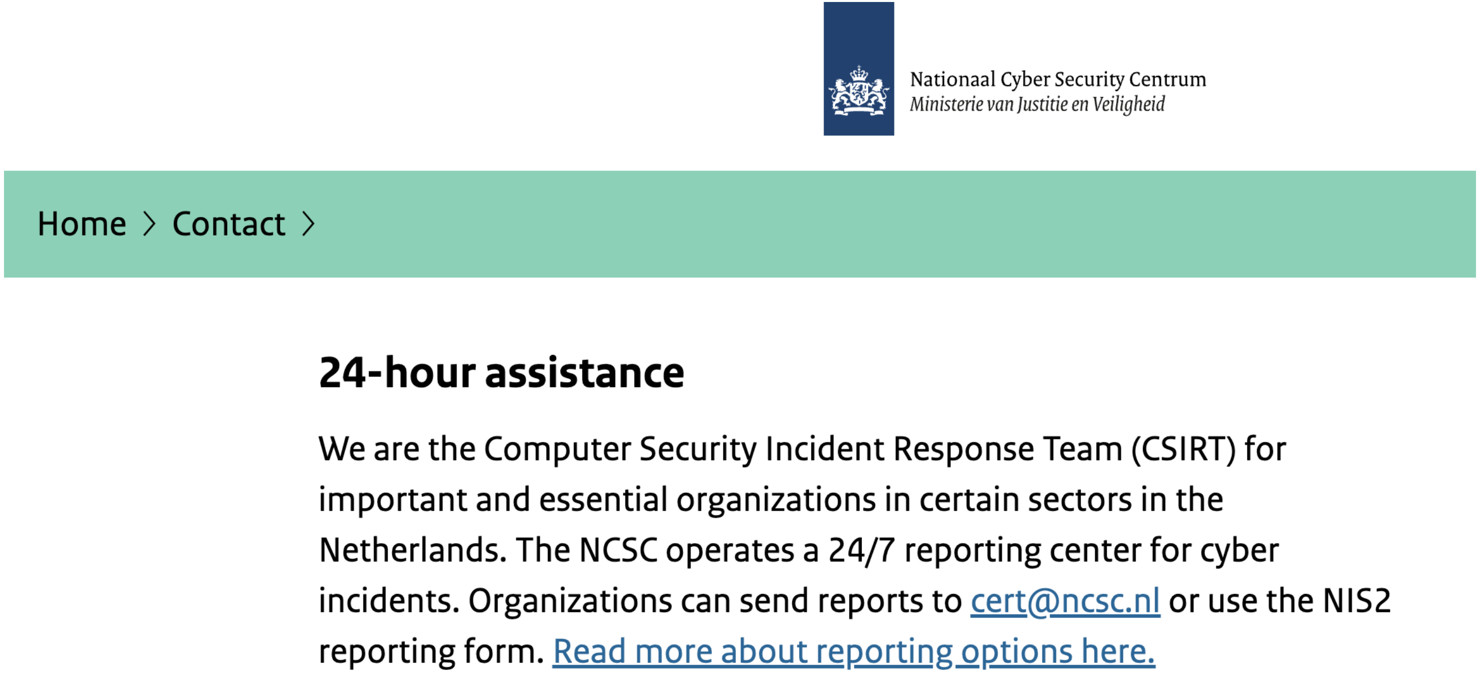
- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]

- Covered by
  - **5.3.6 [VRF-5]**
  - 5.3.7 [VRF-6]
  - 5.4.2 [RMD-1]
  - 5.4.3 [RMD-2]

- **Requirement**:
  - Coordinator involvement is specified in EN ISO/IEC 29147:2020 Clause 5.5.5 and Clause 8.1
- **Input**:
  - Verified report as per [VRF-1]
  - Triaged report as per [VRF-2]
  - Risk-assessed vulnerabilities as per [VRF-3]
  - Remediation plan and FIX as per [RMD-1]
- **Output**:
  - Assignment of coordinator(s) if applicable
- **Assessment**
  - Assignment of coordinator(s) is documented, if applicable.

- **Notes on the state of the art** :
  - EN ISO/IEC 29147:2020
    - Clause 5.5.5 / Clause 8.1
- **CRA references**:
  - (51) 'CSIRT designated as coordinator' means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555.
- **NIS2 reference:**
  - (61) Member States should designate one of its CSIRTs as a coordinator, acting as a trusted intermediary between the reporting natural or legal persons and the manufacturers or providers of ICT products or ICT services, which are likely to be affected by the vulnerability, where necessary.

Example of designated CSIRT in the Netherlands – NCSC-NL



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Home › Contact ›

24-hour assistance

We are the Computer Security Incident Response Team (CSIRT) for important and essential organizations in certain sectors in the Netherlands. The NCSC operates a 24/7 reporting center for cyber incidents. Organizations can send reports to cert@ncsc.nl or use the NIS2 reporting form. Read more about reporting options here.

Source: https://www.ncsc.nl/contact/24-uurs-hulp

5.3.7 [VRF-6] Operational security

VERIFICATION

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]

  - Covered by
    - 5.3.6 [VRF-5]
    - **5.3.7 [VRF-6]**
    - 5.4.2 [RMD-1]
    - 5.4.3 [RMD-2]

- **Requirement**:
  - Operational security involved when receiving and communicating about vulnerabilities as specified in EN ISO/IEC 29147:2020 Clause 6.7 (applied to PRE-4 Secure communication and VRF-4 - On-going communication)
- **Input**:
  - PRE-4 Secure communication
  - VRF-4 On-going communication
  - PRE-1 CVD Policy
- **Output**:
  - Assignment of coordinator(s) if applicable
- **Assessment**
  - List of communication security mechanisms
  - Description of security measures applied in vulnerability handling

- **Notes on the state of the art** :
  - EN ISO/IEC 29147:2020
    - Clause 6.7
- **Examples**:
  - The principle of need to know applied to the vulnerability reports
  - HTTPS communication
  - Email encryption

[VRF] Open discussion / Considerations

❑ As specified by ISO/IEC 29147:2018 5.6.4 Verification: *This phase is often called “triage.”* ***Triage and verification are usually used interchangeably.***

  ❑***OPT1*** *: We may consider merging [VRF-1] and [VRF-2]. Our initial intention was to have validation steps.*

  ❑***OPT2*** *: Alternatively, the other option is to have the [VRF-1] more aligned with ISO/IEC 29147:2018, Section 6.3, Initial Assessment, and move the section to [PRE]* Preparation.

❑Better contextualization of 5.3.4 [VRF-3] Vulnerability Risk Assessment with PT1 with Risk Assessment activities

❑Consideration in moving [VRF-4] / [VRF-5] / [VRF-6] in the preparation phase

5.3 [VRF] VERIFICATION

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

PT3 - Vulnerability Handling – [RMD] REMEDIATION

- [PRE] Preparation
- [RCP] Receipt
- [VRF] Verification
- **[RMD] Remediation**
- [RLS] Release
- [PRP] Post release

Goal:

- Once a vulnerability has been verified and a decision made to address it, remediation may be required, typically involving mitigation controls in the form of a tested patch or security update.

Requirements:

- [RMD-1] Remediation Decision (ISO 30111:2020 Clause 7.1.5 a)
- [RMD-2] Remediation Development (ISO 30111:2020 Clause 7.1.5 b)
- [RMD-3] Remediation Test (ISO 30111:2020 Clause 7.1.5 c)

Customer facing | Risk management | Internal Activities

5.4.2 [RMD-1] Remediation Decision

Remediation

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements,** address and **remediate vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - 5.3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]

- Covered by
  - 5.3.6 [VRF-5]
  - 5.3.7 [VRF-6]
  - **5.4.2 [RMD-1]**
  - 5.4.3 [RMD-2]

- **Requirement**:
  - Essentially, the decision on how to remediate the vulnerability based on EN ISO/IEC 30111:2020 Clause 7.1.5 (a) remediation decision
- **Input**:
  - Result of 5.3.3 [VRF-2] Triage
  - Result of 5.3.4 [VRF-3] Vulnerability Risk Assessment
- **Output**:
  - Documented remediation decision
- **Assessment**
  - Evidence of the decision on how the vulnerability is addressed exists

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.5 (a) Remediation Decision

5.4.3 [RMD-2] Remediation Development

Remediation

- Essential requirement:
  - (2) **In relation to the risks posed to products with digital elements,** address and **remediate vulnerabilities without delay**, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

- Essential requirement:
  - Covered by
    - **5.**3.2 [VRF-1]
    - 5.3.3 [VRF-2]
    - 5.3.4 [VRF-3]
    - 5.3.5 [VRF-4]

- Covered by
  - 5.3.6 [VRF-5]
  - 5.3.7 [VRF-6]
  - 5.4.2 [RMD-1]
  - **5.4.3 [RMD-2]**

- **Requirement**:
  - Essentially, the decision on how to remediate the vulnerability based on EN ISO/IEC 30111:2020 Clause 7.1.5 (b) Produce remediation
- **Input**:
  - Result of 5.4.2 [RMD-1] Remediation Decision
- **Output**:
  - Intermediary remediation, if applicable
  - Full remediation
- **Assessment**
  - Evidence of planned and provided remediations, along with related documentation (patches, fixes, configuration changes)

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.5 (b) Produce remediation

GAP: We could be more specific in the development to separate security and functionality updates in the release notes.

The related requirement has been integrated in RLS

- **[RLS-1-RQ-02]** Where technically feasible, the manufacturer shall provide new security updates separately from functionality updates.

5.4.4 [RMD-3] Remediation Test

Remediation

- Essential requirement:
  - (3) apply effective and regular tests and reviews of the security of the product with digital elements;

- Essential requirement:
  - Covered by
    - **5.4.4 [RMD-4]**

- **Requirement**:
  - Essentially, the capability to test the update produced on EN ISO/IEC 30111:2020 Clause 7.1.5 (c) Test remediation
  - The methodologies needs to be defined and shared in **PT1** standard but still under definition on the interplay
- **Input**:
  - Remediation developed in [RMD-2]
- **Output**:
  - A test report that shows the effectiveness of the remediation
- **Assessment**
  - Evidence on the testing of the remediation

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.5 (c) Test remediation

Note:
This essential requirement is still not covered in this version of the standard. We are still under evaluation:

1. How to cross-reference with PT1 – how to link with the testing activities of the remediation

[RMD] Open discussion / Considerations

- ❑How to cross-reference with PT1 – how to link with the testing activities of the remediation
- ❑What are the minimum testing activities that we should require for the test of the remediation?

5.4 [RMD] REMEDIATION

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

PT3 - Vulnerability Handling – [RLS] RELEASE

- **[PRE] Preparation**
- [RCP] Receipt
- [VRF] Verification
- [RMD] Remediation
- **[RLS] Release**
- [PRP] Post release

Goal:

- This phase includes deploying remediation, describing associated changes, and sharing information with relevant stakeholders.

Requirements:

- [RLS-1] Provisioning of Security Updates (ISO 30111:2020 Clause 7.1.6 a)
- [RLS-2] Distribute of security update
- [RLS-3] Release Information (EN ISO/IEC 29147:2020 Clause 7.4 / 7.5 / 7.6 / 7.7)

🟨 Customer facing 🟦 Risk management 🟩 Internal Activities

5.5.2 [RLS-1] Provisioning of Security Updates

Release

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

- Essential requirement:
  - Covered by
    - **5.5.2 [RLS-1]**

- **Requirement**:
  - Essentially, the capability to provide security updates according to EN ISO/IEC 30111:2020 Clause 7.1.6 Release and 5.4.4 [RMD-3] Remediation Test
  - Allowing Integrity and authenticity
  - Separation between security and functionality update
- **Input**:
  - Results of 5.3.4 [VRF-3] Vulnerability Risk Assessment
  - Remediation tested as per 5.4.4 [RMD-3] Remediation Test
- **Output**:
  - Security patch/update and authenticity protection
- **Assessment**
  - Evidence on software update authenticity
  - Justification in case the security update is not separated from functionality

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.6 Release

Note:
There is a requirement, RLS-1-RQ-02, that should be moved under 5.4.3 [RMD-2] Remediation Development.

- [RLS-1-RQ-02] Where technically feasible, the manufacturer shall provide new security updates separately from functionality updates.

5.5.3 [RLS-2] Distribution of security updates

Release

- Essential requirement:
  - (7) **provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;**

- Essential requirement:
  - Covered by
    - **5.5.3 [RLS-2]**

- **Requirement**:
  - Distribution without delay of the security update
  - Secure distribution (such as encryption, hash, digital signature, certificate)
  - Where applicable, have automatic updates
- **Input**:
  - Remediation tested as per 5.4.4 [RMD-3] Remediation Test
- **Output**:
  - Evidence of the distribution of the security update in a secure manner
  - Justification for not using the automatic update if not used
- **Assessment**
  - Evidence on secure update distribution and related implementation

- **Notes on the state of the art** :
  - NCSC – Device security principles for manufacturers (LINK)
    - ETSI EN 303 645 5.3-7, 5.3-9 and 5.3-10
    - NIST information on digital signatures
    - NIST information on Message Authentication Codes
    - NIST SP 800-131A
    - NIST FIPS 140-3
    - NIST SP 800-213A: Data Protection – Cryptographic Capabilities and Support

5.5.4 [RLS-3] Release Information

Release

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

- Essential requirement:
  - Covered by
    - 5.1.6 [PRE-5]
    - **5.5.4 [RLS-3]**

- **Requirement**:
  - Release the information about the fixed vulnerabilities along with (description of vulnerability, product identification, impact, severity, and remediation instructions)
- **Input**:
  - Remediation tested as per 5.4.4 [RMD-3] Remediation Test
- **Output**:
  - Evidence on secure update distribution and related implementation, and related public information
- **Assessment**
  - Consistency in the information shared and alignment within the internal process

- **Notes on the state of the art** :
  - ISO/IEC 20153:2025: Information technology - OASIS Common Security Advisory Framework (CSAF) v2.0 Specification
- **Example**:
  - Fortinet's resolution of CVE-2024-47575 with FG-IR-24-423
  - SolarWinds Advisories for SUNBURST / SUPERNOVA
    - FAQ
    - CISA Advisory (AA20-352A)

[RLS] Open discussion / Considerations

❑ To which detail can we specify how to define **timely** (for sure based on Risk assessment), but at what level can we define it in a way that does not disrupt verticals and specific domains?

5.5 [RLS] RELEASE

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

PT3 - Vulnerability Handling – [PRP] POST RELEASE

- [PRE] Preparation
- [RCP] Receipt
- [VRF] Verification
- [RMD] Remediation
- [RLS] Release
- **[PRP] Post release**

Goal:

- This phase includes monitoring of the released update. Lessons learned and reflections during the post-release may even lead to changes and improvements in the development process.

Requirements:

- [PRP-1] Post release plan (ISO 30111:2020 Clause 7.1.7)

Customer facing	Risk management	Internal Activities

5.5.2 [PRP-1] POST RELEASE PLAN

POST RELEASE

- Essential requirement:
  - N/A

- Essential requirement:
  - 5.5.2 [PRP-1]

- **Requirement**:
  - Essentially, the root cause analysis and reflections contained in EN ISO/IEC 30111:2020 Clause 7.1.7 Post-release to prevent future occurrence of an already identified and confirmed vulnerability
- **Input**:
  - Results of 5.3.4 [VRF-3] Vulnerability Risk Assessment
  - Remediation tested as per 5.4.4 [RMD-3] Remediation Test
- **Output**:
  - Post-release action plan
- **Assessment**
  - Evidence of post release action plan exists.

- **Notes on the state of the art** :
  - EN ISO/IEC 30111:2020
    - Clause 7.1.7 Post-release

Note:
This action should be present to make sure that manufacturers are learning from the vulnerabilities and after a reactive approach in solving the issues they should be able to identify root cause and trigger improvements of their internal process

[PRP] Open discussion / Considerations

❑Do we need to add something additional or more specific? What does the industry need here?

5.5 [PRP] POST-RELEASE

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

ANNEX ZA: Overview of the ESR covered

(1) **identify and document** vulnerabilities **and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;**	– **Covered by** – 5.1.7 [PRE-6] – 5.1.8 [PRE-7] – 5.1.9 [PRE-8] – 5.2.2 [RCP-1] – 5.2.3 [RCP-2] – 5.2.4 [RCP-3]
(2) **In relation to the risks posed to products with digital elements, address** and remediate **vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;**	– **Covered by** – 5.3.2 [VRF-1] – 5.3.3 [VRF-2] – 5.3.4 [VRF-3] – 5.3.5 [VRF-4] – 5.3.6 [VRF-5] – 5.3.7 [VRF-6] – 5.4.2 [RMD-1] – 5.4.3 [RMD-2]
(3) apply effective and regular tests and reviews of the security of the product with digital elements;	– **Covered by** – 5.4.4 [RMD-4]
(4) **once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;**	– **Covered by** – 5.1.6 [PRE-5] – 5.5.4 [RLS-3]

ANNEX ZA: Overview of the ESR covered

(5) put in place and enforce a policy on coordinated vulnerability disclosure;	– **Covered by** – 5.1.2 [PRE-1]
(6) **take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements**;	– **Covered by** – 5.1.3 [PRE-2] – 5.1.4 [PRE-3] – 5.1.5 [PRE-4]
(7) **provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;**	– **Covered by** – 5.5.3 [RLS-2]
(8) **ensure that, where security updates are available to address identified security issues, they are disseminated without delay and,** unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	– **Covered by** – 5.5.2 [RLS-1]
– N/A	– **Covered by** – 5.5.2 [PRP-1]

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)

Post-Workshop Survey: Cyber Resilience Act - Vulnerability Handling

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

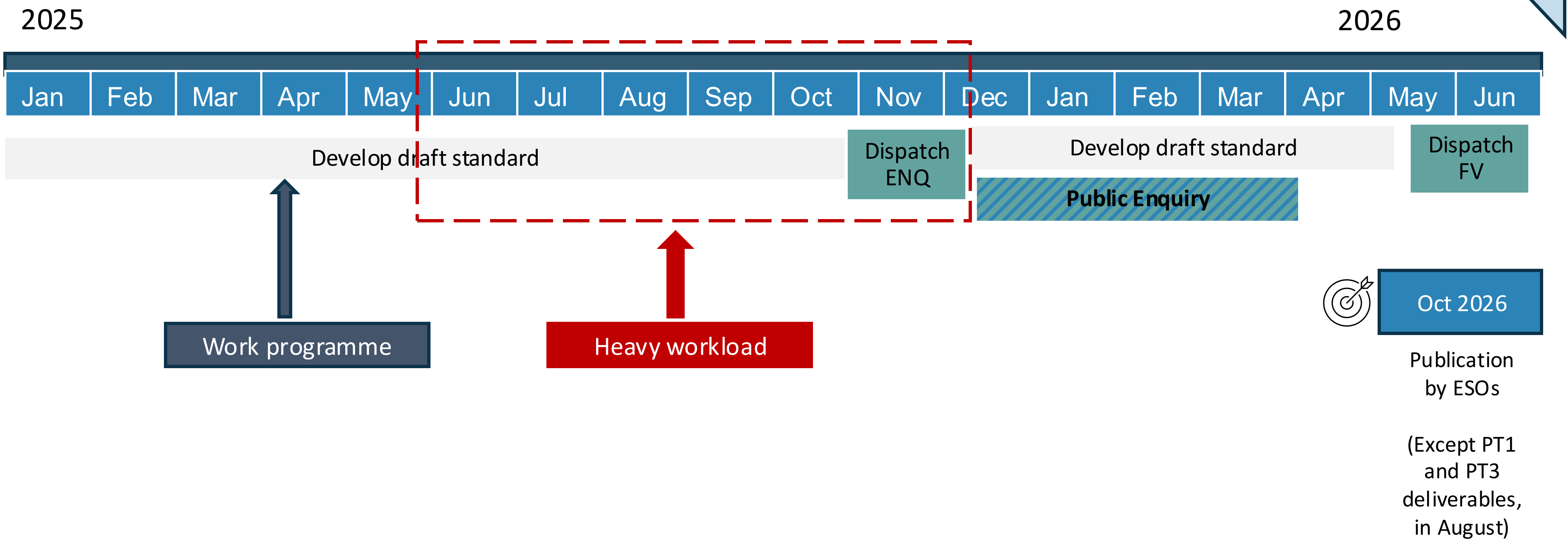
Vulnir

Thank you

VULNIR.com

info@vulnir.com

High level expected timeline



2025

2026

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun

Develop draft standard

Dispatch ENQ

Develop draft standard

Public Enquiry

Dispatch FV

Work programme

Heavy workload

Oct 2026

Publication by ESOs

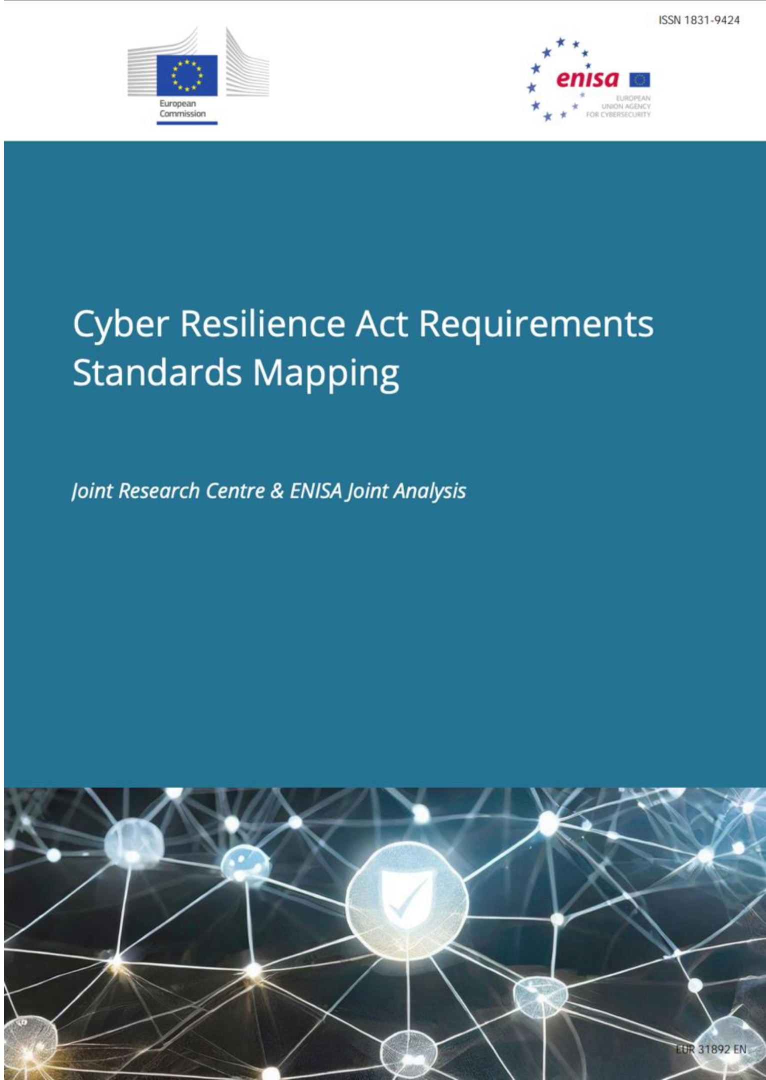
(Except PT1 and PT3 deliverables, in August)

***Reference**: How to write a winning SSP application: focus on SSP#7 topics - Date: 2025-06-12 – **source:** CYBERSTAND / CENELEC.*

Gaps identified

- (1) Risk assessment not specific to the system or product design
- (2) Find the right balance in the assessment for the no known exploitable vulnerabilities (Common Criteria vs ETSI EN 303 645)
- (3 a) The particular use of non-erasable memories for configuration management is not covered.
- (3 f) More detailed guidance on the implementation of availability principles for generic user products
- (3 h) Lack of concrete requirements targeting the attack surface minimisation
- (3 i) some aspects of defence in depth, sandboxing, and certain mitigation techniques might not be explicitly covered by the selected standards
- (3 k) Do not explicitly cover the requirement of notifying users about the availability of updates.

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



ISSN 1831-9424

European Commission

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cyber Resilience Act Requirements Standards Mapping

Joint Research Centre & ENISA Joint Analysis

EUR 31892 EN

Development

Discovery

Validation

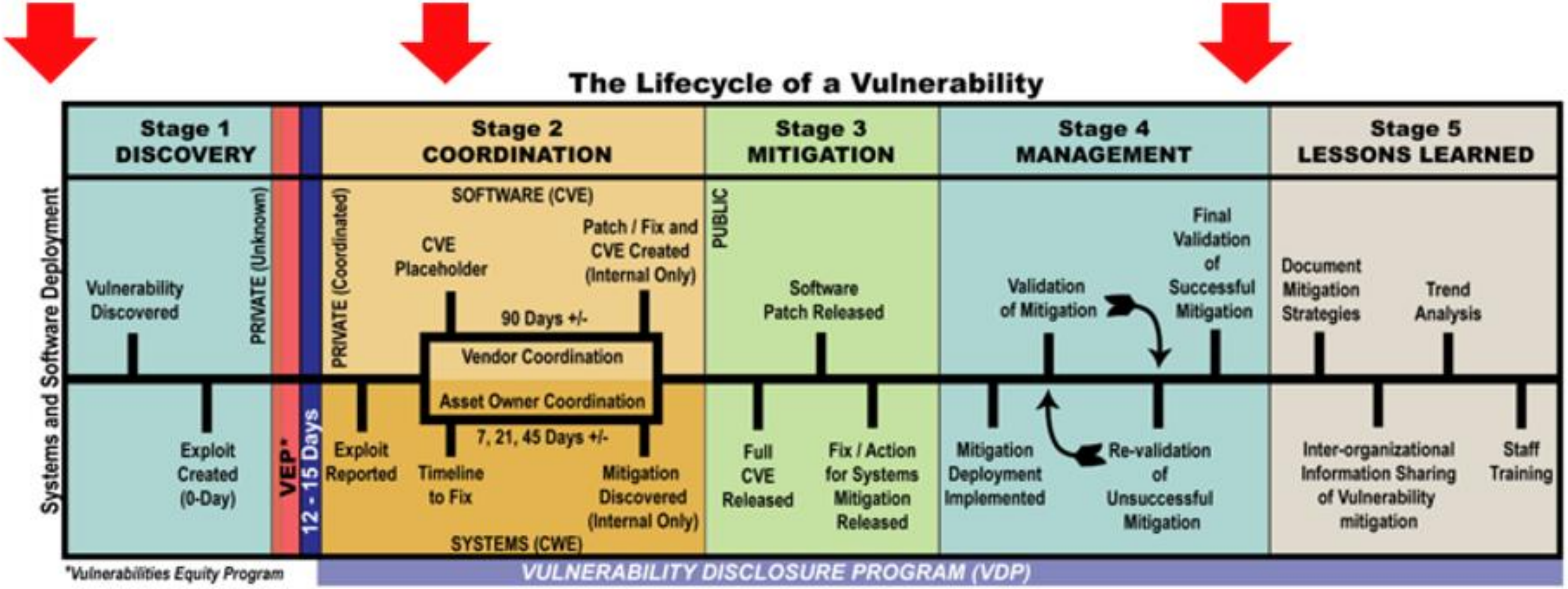

The Lifecycle of a Vulnerability
Stage 1
DISCOVERY
Stage 2
COORDINATION
Stage 3
MITIGATION
Stage 4
MANAGEMENT
Stage 5
LESSONS LEARNED
Systems and Software Deployment
Vulnerability Discovered
Exploit Created (0-Day)
PRIVATE (Unknown)
VEP*
12 - 15 Days
PRIVATE (Coordinated)
SOFTWARE (CVE)
CVE Placeholder
Patch / Fix and CVE Created (Internal Only)
90 Days +/-
Vendor Coordination
Asset Owner Coordination
7, 21, 45 Days +/-
Exploit Reported
Timeline to Fix
Mitigation Discovered (Internal Only)
SYSTEMS (CWE)
PUBLIC
Software Patch Released
Full CVE Released
Fix / Action for Systems Mitigation Released
Validation of Mitigation
Final Validation of Successful Mitigation
Mitigation Deployment Implemented
Re-validation of Unsuccessful Mitigation
Document Mitigation Strategies
Trend Analysis
Inter-organizational Information Sharing of Vulnerability mitigation
Staff Training
*Vulnerabilities Equity Program
VULNERABILITY DISCLOSURE PROGRAM (VDP)

Figure 2: Stages for Using a Bug Bounty

***Reference**:* [*https://thescif.org/lifecycle-of-a-vulnerability-overview-part-2-5bf86e622abd*](https://thescif.org/lifecycle-of-a-vulnerability-overview-part-2-5bf86e622abd)

ISO/IEC 30111:2019 Crosswalk

30111	Sub-Clause	
7.1.1 General		
7.1.2 Preparation		
7.1.3 Receipt	a) Internally Found Vulnerabilities	5.2.2 [RCP-1]
	b) Externally Found Vulnerabilities	5.2.2 [RCP-1]
	c) Publicly Disclosed Vulnerabilities	5.2.2 [RCP-1]

ISO/IEC 30111:2019 Crosswalk

30111	Sub-Clause	
7.1.4 Verification	a) Initial Investigation	5.3.2 [VRF-1] / 5.3.3 [VRF-2]
	b) Possible Process Exit 1) Duplicate	5.3.2 [VRF-1] / 5.3.3 [VRF-2]
	b) Possible Process Exit 2) Obsolete product	5.3.2 [VRF-1] / 5.3.3 [VRF-2]
	b) Possible Process Exit 3) Non-security	5.3.2 [VRF-1] / 5.3.3 [VRF-2]
	b) Possible Process Exit 4) Other vendor	5.3.2 [VRF-1] / 5.3.3 [VRF-2]
	c) Root Cause Analysis	5.5.2 [PRP-1]

ISO/IEC 30111:2019 Crosswalk

30111	Sub-Clause	
7.1.4 Verification	d) Further investigation	
	e) Prioritization	5.3.2 [VRF-1] / 5.3.3 [VRF-3]
	f) Inform reporter	
7.1.5 Remediation Development	a) Remediation decision	5.4.2 [RMD-1]
	b) Produce remediation	5.4.3 [RMD-2]
	c) Test remediation	5.4.4 [RMD-3]
7.1.6 Release		5.5.2 [RLS-1]
7.1.7 Post-release	all	5.5.2 [PRP-1]

ISO/IEC 30111:2019 Crosswalk

30111	Sub-Clause
7.2 Process Monitoring	all
7.3 Confidentiality	-
8 Supply chain considerations	

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause
5.6 Vulnerability Handling Process Summary	5.6.1 General 5.6.2 Preparation 5.6.3 Receipt 5.6.4 Verification 5.6.5 Remediation development 5.6.6 Release 5.6.7 Post-release
	5.6.8 Embargo period
5.7 Information exchange during vulnerability disclosure	send-report-to
	release-advisory-to

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause	
5.8 Confidentiality	5.8.2 Secure communication	5.1.5 [PRE-4]
5.9 Vulnerability advisories		
5.10 Vulnerability exploitation		
5.11 Vulnerabilities and risk		

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause	
6 Receiving vulnerability reports	6.1 General	
	6.2.2 Capability to receive reports	5.1.3 [PRE-2]
	6.2.3 Monitoring	5.2.2 [RCP-1]
	6.2.4 Report Tracking	
	6.2.5 Report Acknowledgement	
6.3 Initial assessment		
6.4 Further investigation		

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause	
6.5 On-going communication		5.3.5 [VRF-4]
6.6 Coordinator involvement		
6.7 Operational security		5.3.7 [VRF-6]
7 Publishing vulnerability advisories	all	
	7.3 Advisory publication timing	
	7.4 Advisory elements	5.5.4 [RLS-3]
	7.5 Advisory communication	5.5.4 [RLS-3]

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause	
	7.6 Advisory format	5.5.4 [RLS-3]
	7.7 Advisory authenticity	5.5.4 [RLS-3]
	7.8 Remediations	
	all	
8 Coordination	8.1 General	5.3.6 [VRF-5]
	8.2 Vendors playing multiple roles	

ISO/IEC 29147:2018 Crosswalk

ISO/IEC 29147:2018	Sub-Clause	
9 Vulnerability disclosure policy	all	5.1.2 [PRE-1]
	9.2.2 Preferred contact mechanism	5.1.2 [PRE-1] / 5.1.4 [PRE-3]
	9.3.2 Vulnerability report contents	5.1.2 [PRE-1]
	9.3.3 Secure communication options	5.1.2 [PRE-1] / 5.1.5 [PRE-4]
	9.3.4 Setting communication expectations	5.1.2 [PRE-1]
	9.3.6 Publication	5.1.2 [PRE-1]
	9.4.3 Disclosure timeline	5.1.2 [PRE-1]