Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Open-Source Cyber Resilience Act Tools (OSCRAT)

Introductory CRA & Project Training Content

DIGITAL-ECCC-2024-DEPLOY-CYBER-06-COMPLIANCECRA
Tools for compliance with CRA requirements and obligations

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by
the European Union

Definition

- ***Product with digital elements*** means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately
- ***Horizontal standards*** - i.e., not targeting a specific use case or a market sector/product - emerged as the most relevant to cover the purposes of the different requirements.
- ***Remote data processing*** means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions
- ***Critical product*** means a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III
- ***CE marking*** It's a mark from a manufacturer showing their product meets essential requirements in EU law for digital elements and processes, allowing it to be marketed
- ***Conformity assessment*** means the process of verifying whether the essential requirements set out in Annex I have been fulfilled
- ***Self-assessment*** *t*he manufacturer himself ensures the conformity of the products to the legislative requirements.
- ***Third-party assessment*** are laboratories, inspection and certification bodies which are known generally as conformity assessment bodies, or more formally as “Notified Bodies”
- ***Notified body*** means a conformity assessment body designated in accordance with Article 33 of this Regulation and other relevant Union harmonisation legislation
- ***Distributor*** means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties
- ***Importer*** means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union

CRA Elements

- **Cybersecurity rules** for hardware and software for placing on the EU market
- **Obligations** for hardware manufacturers, software developers, importers, distributors and resellers
- Cybersecurity **essential requirements** across the life cycle (5 years)
- Harmonized **standards** to follow and **Horizontal** Standardization Framework
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**

CRA Scope

Digital elements:

- ✓ **Hardware products** and components, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- ✓ **Software products** and components, such as OS, word processing, games or mobile apps
- ✓ "**Products with digital elements**" also includes **remote data processing solutions**

Not covered:

- ✗ **Non-commercial projects, including open source** if a project is not part of a commercial activity
- ✗ **Services**, such **cloud/SaaS** – unless as "*remote data processing*"

Outright exclusions:

- ✗ **Certain products regulated on cybersecurity** (cars, medical devices, in vitro, certified aeronautical equipment) under the new and old approach

CRA Categorize Products

Unclassified / Default

- The Default category applies to products without critical cybersecurity vulnerabilities.

- Vulnerability self-assessment.

- Example: photo-editing software, video games, and other commonplace software and devices.

Class I

- Must adhere to the application of a standard or

- Third-party assessment to demonstrate conformity.

Class II

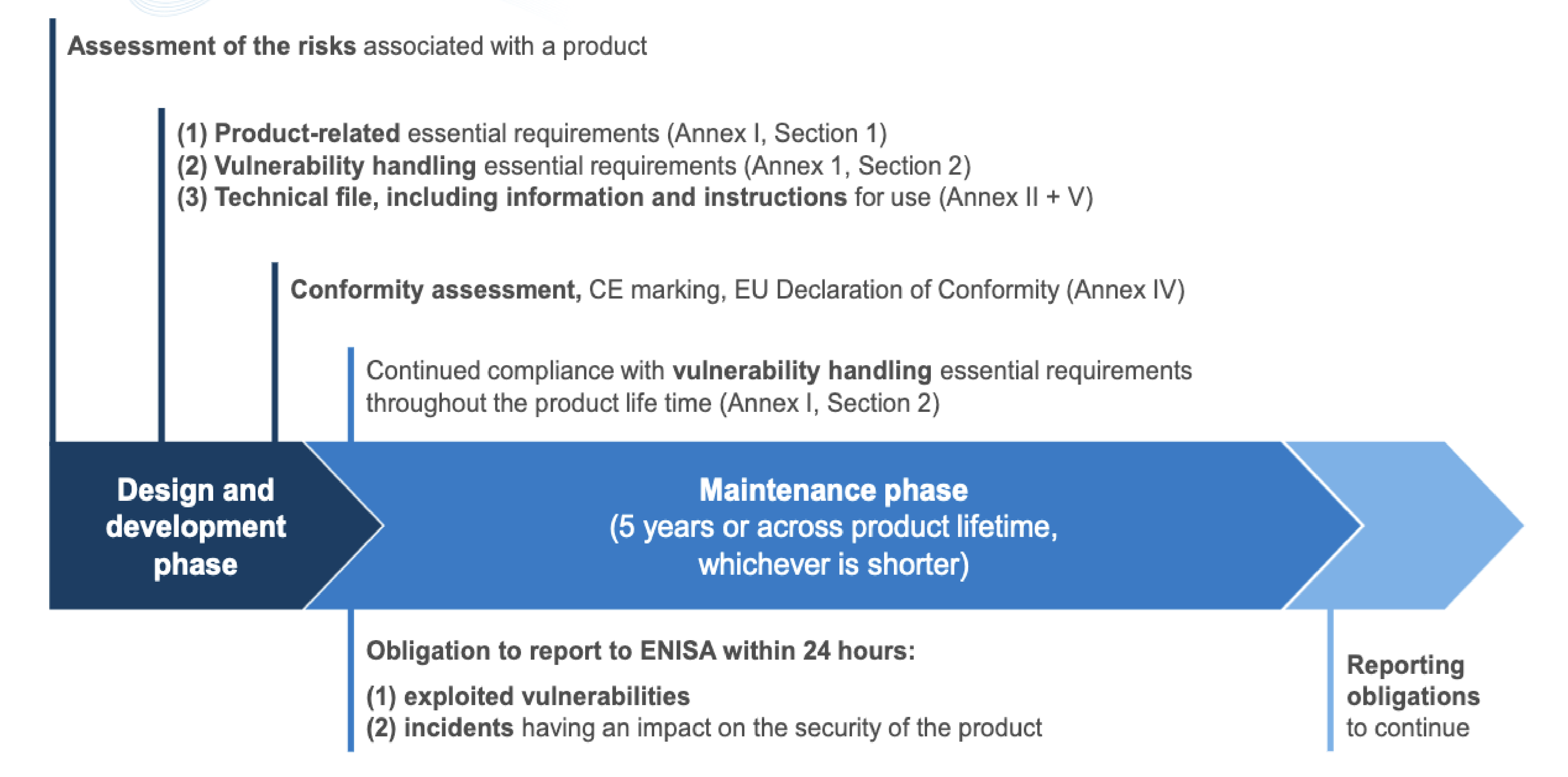
- Must complete a third-party conformity assessment.

- Annex III of the CRA splits critical products into modules: B, C, & H.

Class I and Class II based on their level of risk

- Whether it runs with privilege, privileged access, or performs a function critical to trust
- Whether it is to be used in sensitive environments as described by NIS2
- Whether it is to be used to process personal information or other sensitive functions
- Whether its vulnerability can affect a plurality of people
- Whether it has already caused adverse effects when disrupted

CRA - Obligations



Assessment of the risks associated with a product

(1) **Product-related** essential requirements (Annex I, Section 1)
(2) **Vulnerability handling** essential requirements (Annex 1, Section 2)
(3) **Technical file, including information and instructions** for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

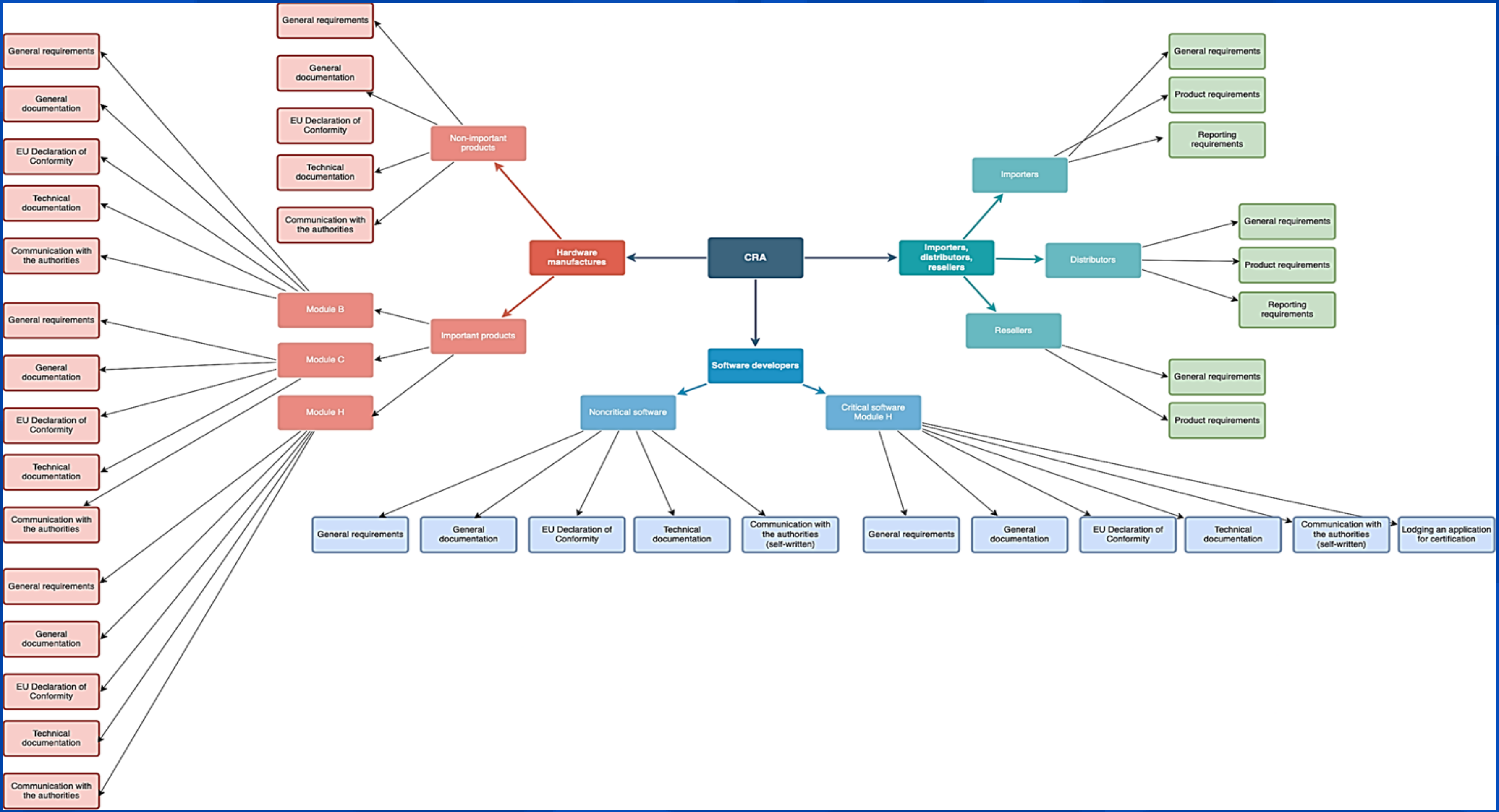
Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) **exploited vulnerabilities**
(2) **incidents** having an impact on the security of the product

Reporting obligations to continue

CRA in a Nutshell



CRA

Hardware manufactures

Non-important products

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities

Important products

Module B

Module C

Module H

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities

Software developers

Noncritical software

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities (self-written)

Critical software Module H

General requirements

General documentation

EU Declaration of Conformity

Technical documentation

Communication with the authorities (self-written)

Lodging an application for certification

Importers, distributors, resellers

Importers

General requirements

Product requirements

Reporting requirements

Distributors

General requirements

Product requirements

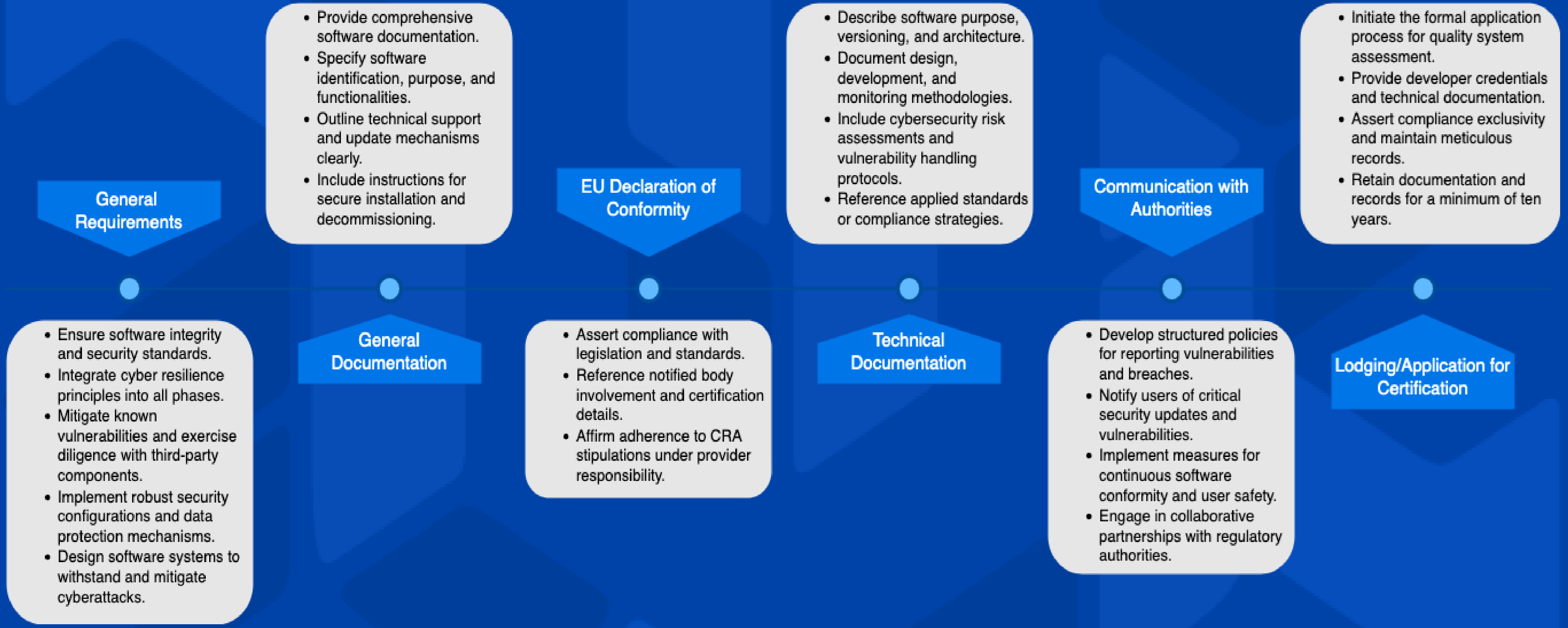
Reporting requirements

Resellers

General requirements

Product requirements

CRA Essential Requirements



General Requirements

- Ensure software integrity and security standards.
- Integrate cyber resilience principles into all phases.
- Mitigate known vulnerabilities and exercise diligence with third-party components.
- Implement robust security configurations and data protection mechanisms.
- Design software systems to withstand and mitigate cyberattacks.

General Documentation

- Provide comprehensive software documentation.
- Specify software identification, purpose, and functionalities.
- Outline technical support and update mechanisms clearly.
- Include instructions for secure installation and decommissioning.

EU Declaration of Conformity

- Assert compliance with legislation and standards.
- Reference notified body involvement and certification details.
- Affirm adherence to CRA stipulations under provider responsibility.

Technical Documentation

- Describe software purpose, versioning, and architecture.
- Document design, development, and monitoring methodologies.
- Include cybersecurity risk assessments and vulnerability handling protocols.
- Reference applied standards or compliance strategies.

Communication with Authorities

- Develop structured policies for reporting vulnerabilities and breaches.
- Notify users of critical security updates and vulnerabilities.
- Implement measures for continuous software conformity and user safety.
- Engage in collaborative partnerships with regulatory authorities.

Lodging/Application for Certification

- Initiate the formal application process for quality system assessment.
- Provide developer credentials and technical documentation.
- Assert compliance exclusivity and maintain meticulous records.
- Retain documentation and records for a minimum of ten years.

How To Get Compliant

Hardware Manufacturers				Software Developers		Importers/ Distributors / Resellers
Non-important	Important			Non-critical	Critical	
	Module B	Module C	Module H			
- Class I if mets specific criteria can be self-assessed - Class II self-assessed - Notified body assessment	- Hardware Examination - No Quality System Requirement	- Self-assessed based on previous certificate products based on module B - New assessment by a Notified body	- Quality System Evaluation - Rigorous Process Assessment - Assessed by the Notified body	- Self assessment or Notified body assess - Critical product Annex III - Notified Body Oversight - Flexibility	- Notified body assessment - Module H assessment - Quality System evaluation - Notified Body Oversight - Critical product Annex III	- Compliance with essential requirements Annex I - Conformity Assessment procedures - Technical documentation and CE marking - Contact information and user-friendly instructions

Hardware Manufacturers Requirements Checklist

	Important products			Non-Important products
	Module B	Module C	Module H	
General	✓ Assessed by notified body	✓ Self-assessed, based on previous EU-type examination certification for the same type of product (Module B)	✓ Assessed by notified body ✓ Clear written policies ✓ Procedures and instructions	✓ Self-assessed
General Documentation	✓ Self-written	✓ Self-written	✓ Self-written	✓ Self-written
EU Declaration of Conformity	✓ Self-written	✓ Self-written	✓ Self-written	✓ Self-written
Technical Documentation	✓ Self-written ✓ Assessed by notified body	✓ Self-written ✓ Assessed by notified body	✓ Self-written ✓ Assessed by notified body	✓ Self-written
Authorities Communication	✓ Self-written	✓ Self-written	✓ Self-written	✓ Self-written
Lodging for Certification	✓ Maintain quality system documentation	✓ Not Applicable	✓ Maintain quality system documentation	✓ Not Applicable

Software Developers Requirements Checklist

Critical Software (H)

General

- ✓ Assessed by notified body
- ✓ Clear written policies
- ✓ Procedures and instructions

General Documentation

- ✓ Self-written

EU Declaration of Conformity

- ✓ Self-written

Technical Documentation

- ✓ Self-written
- ✓ Assessed by notified body

Authorities Communication

- ✓ Self-written

Lodging for Certification

- ✓ Maintain quality system documentation

Non-Critical Software

General

- ✓ Self-assessed

General Documentation

- ✓ Self-written

EU Declaration of Conformity

- ✓ Self-written

Technical Documentation

- ✓ Self-written

Authorities Communication

- ✓ Self-written

Importers / Distributors / Resellers Requirements Checklist

Importers

General

- ✓ Do not Modify Products

Product

- ✓ Compliance with Essential Req.
- ✓ Conformity Assessment Procedures
- ✓ Technical Documentation
- ✓ CE Marking
- ✓ Contact and Accompanying Information

Reporting

- ✓ Cooperation with Authorities
- ✓ Non-Conformity Reporting
- ✓ Documentation Retention
- ✓ Information Provision
- ✓ Manufacturer Ceases Operations

Distributors

General

- ✓ Product Modification
- ✓ Due Care

Product

- ✓ CE Marking Verification
- ✓ Compliance Verification

Reporting

- ✓ Cooperation with Authorities
- ✓ Non-Conformity Reporting
- ✓ Information Provision
- ✓ Manufacturer Ceases Operations

Resellers

General

- ✓ Product Modification

Reporting

- ✓ Cooperation with Authorities
- ✓ Information Provision
- ✓ Record Keeping

Mapping CRA Requirements Against Cyber Security Standards

- The widely used ISO/IEC 27001 (information security management);
- ISO/IEC 27002 (information security controls);
- ISO/IEC 27402 (DIS) (IoT device baseline requirements);
- ETSI EN 303 645 (IoT consumer products);
- ETSI TS 103 732 (consumer mobile device);
- ETSI TS 103 848 (home gateway products);
- The EN IEC 62443 series of standards for electronically secure industrial automation and control systems (IACS);
- ISO/IEC 29147 and 30111 (vulnerability disclosure and handling);
- The ISO/IEC 27036 series for supply chain security;
- ISO/IEC 27034 (application security);
- The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408);

Essential Tools to Facilitate CRA for SMEs (1)

1. Compliance Assessment and Gap Analysis Tools

Automated tools that assess SMEs' current cybersecurity posture, identify gaps in compliance with CRA requirements, and provide recommendations for remediation.

2. Compliance Checklist Generators

User-friendly tools that generate customized checklists based on SMEs' specific industry, size, and regulatory obligations under the CRA, guiding them through the compliance process step-by-step.

3. Policy and Procedure Templates

Pre-designed templates for developing essential CRA compliance policies, procedures, and documentation tailored to SMEs' needs, saving time and resources in creating these foundational documents

4. Risk Management Platforms

Integrated risk management solutions that help SMEs identify, assess, prioritize, and mitigate cybersecurity risks in alignment with CRA requirements, providing a structured approach to risk management.

5. Vulnerability Scanning and Patch Management Tools

Automated vulnerability scanning tools that detect and prioritize security vulnerabilities within SMEs' IT infrastructure and applications, along with patch management capabilities to facilitate timely remediation.

6. Compliance Documentation Automation Platforms

Platforms that streamline the creation, organization, and maintenance of CRA compliance documentation for SMEs, offering templates, version control, and document management functionalities to ensure regulatory adherence.

Essential Tools to Facilitate CRA for SMEs (2)

7. Security Awareness Training Modules

Interactive e-learning modules and training materials focused on educating SME employees about cybersecurity best practices, CRA compliance obligations, and threat awareness to foster a security-conscious culture.

8. Incident Response Planning Software

Incident response planning tools that guide SMEs through the development of comprehensive incident response plans, including workflows, communication protocols, and escalation procedures, to effectively respond to cybersecurity incidents.

9. Security Configuration Management Solutions

Tools that automate the configuration and hardening of SMEs' IT systems and network devices according to CRA-prescribed security standards and best practices, reducing the risk of misconfigurations and unauthorized access.

10. Continuous Monitoring and Reporting Dashboards

Real-time monitoring dashboards that provide SMEs with visibility into their cybersecurity posture, compliance status, and ongoing performance against CRA requirements, enabling proactive risk management and reporting.

OSCRAT Tools to Facilitate CRA for SMEs

☑️ 1. Compliance Assessment Checklist and Gap Analysis Tools

Automated tools that assess SMEs' current cybersecurity posture, identify gaps in compliance with CRA requirements, and provide recommendations for remediation and guiding SMEs through the compliance process step-by-step.

2. Incident Response and Reporting

Incident response planning tools that guide SMEs through the development of comprehensive incident response plans, including workflows, communication protocols, and escalation procedures, to effectively respond to cybersecurity incidents.

⚠️ 3. Vulnerability Scanning and Patch Management Tools

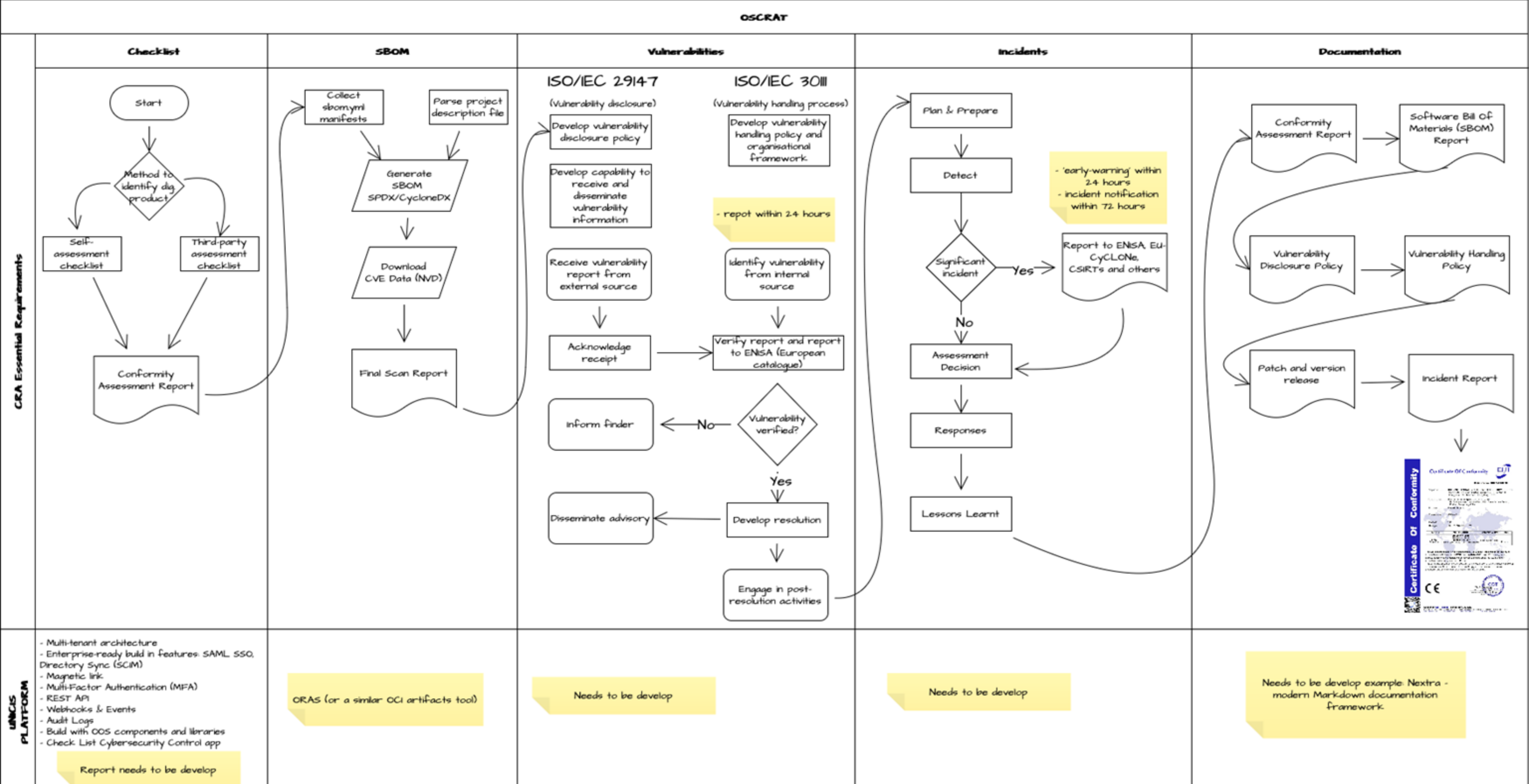
Automated vulnerability scanning OOS tools that detect and prioritize security vulnerabilities within SMEs' IT infrastructure and applications, along with patch management capabilities to facilitate timely remediation and reporting to authorities in 24 hours.

4. Software bill of materials (SBOM) Generation

Automates the creation of SBOMs by scanning software components and dependencies within the SME's IT infrastructure. It compiles detailed inventories of software components, including version numbers, dependencies, and licensing information using the SPDX & CycloneDX standards.

5. Documentation and Certificate of Conformity

OSCRAT Tools for CRA



OSCRAT

CRA Essential Requirements

Checklist

Start

Method to identify dig. product

Self-assessment checklist

Third-party assessment checklist

Conformity Assessment Report

SBOM

Collect sbom.yml manifests

Parse project description file

Generate SBOM SPDX/CycloneDX

Download CVE Data (NVD)

Final Scan Report

Vulnerabilities

ISO/IEC 29147 (Vulnerability disclosure)

Develop vulnerability disclosure policy

Develop capability to receive and disseminate vulnerability information

Receive vulnerability report from external source

Acknowledge receipt

Inform finder

Disseminate advisory

ISO/IEC 30111 (Vulnerability handing process)

Develop vulnerability handing policy and organisational framework

- repot within 24 hours

Identify vulnerability from internal source

Verify report and report to ENISA (European catalogue)

Vulnerability verified?

No

Yes

Develop resolution

Engage in post-resolution activities

Incidents

Plan & Prepare

Detect

- 'early-warning' within 24 hours
- incident notification within 72 hours

Significant incident

Yes

No

Report to ENISA, EU-CyCLONe, CSIRTs and others

Assessment Decision

Responses

Lessons Learnt

Documentation

Conformity Assessment Report

Software Bill Of Materials (SBOM) Report

Vulnerability Disclosure Policy

Vulnerability Handing Policy

Patch and version release

Incident Report

UNICIS PLATFORM

- Multi-tenant architecture
- Enterprise-ready build in features: SAML SSO, Directory Sync (SCIM)
- Magnetic link
- Multi-Factor Authentication (MFA)
- REST API
- Webhooks & Events
- Audit Logs
- Build with OOS components and libraries
- Check List Cybersecurity Control app

Report needs to be develop

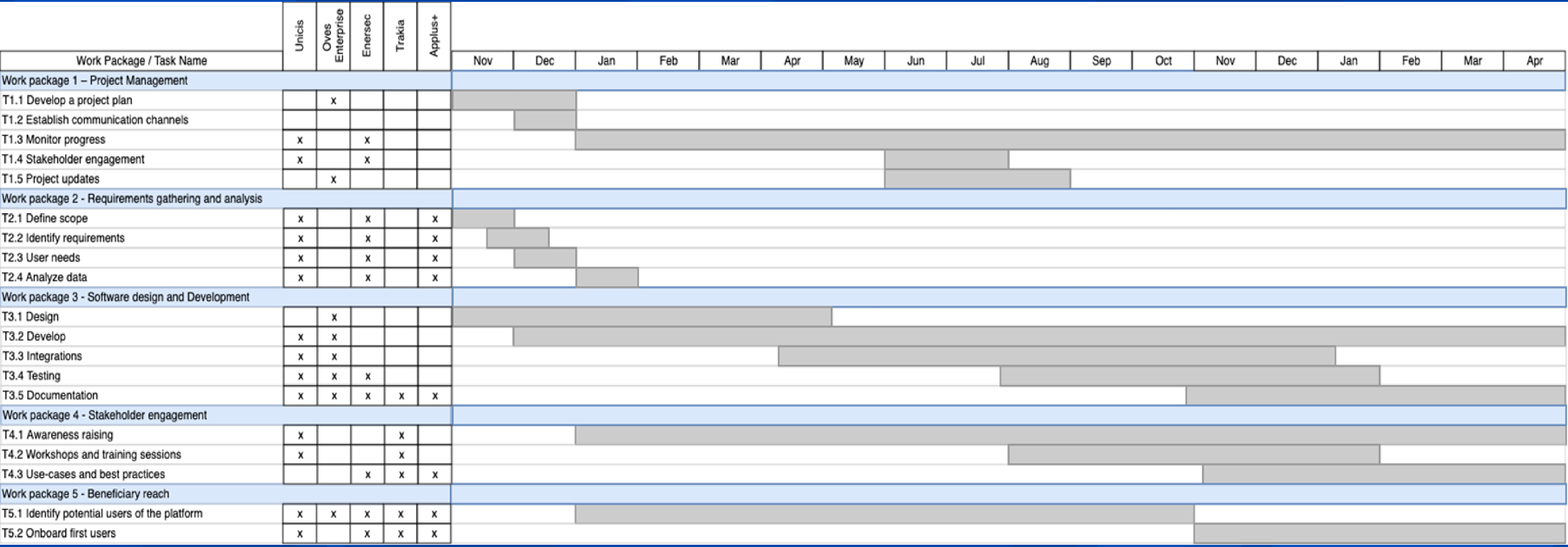
ORAS (or a similar OCI artifacts tool)

Needs to be develop

Needs to be develop

Needs to be develop example: Nextra - modern Markdown documentation framework

Project Working Packages Gantt



Work Package / Task Name	Unicis	Oves Enterprise	Enersec	Trakia	Applus+	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
Work package 1 – Project Management																							
T1.1 Develop a project plan		x				▨	▨																
T1.2 Establish communication channels							▨																
T1.3 Monitor progress	x		x					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
T1.4 Stakeholder engagement	x		x										▨	▨									
T1.5 Project updates		x											▨	▨	▨								
Work package 2 - Requirements gathering and analysis																							
T2.1 Define scope	x		x		x	▨																	
T2.2 Identify requirements	x		x		x	▨	▨																
T2.3 User needs	x		x		x		▨																
T2.4 Analyze data	x		x		x			▨															
Work package 3 - Software design and Development																							
T3.1 Design		x				▨	▨	▨	▨	▨	▨												
T3.2 Develop	x	x					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
T3.3 Integrations	x	x									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨			
T3.4 Testing	x	x	x												▨	▨	▨	▨	▨	▨			
T3.5 Documentation	x	x	x	x	x													▨	▨	▨	▨	▨	▨
Work package 4 - Stakeholder engagement																							
T4.1 Awareness raising	x			x				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
T4.2 Workshops and training sessions	x			x											▨	▨	▨	▨	▨	▨			
T4.3 Use-cases and best practices			x	x	x													▨	▨	▨	▨	▨	▨
Work package 5 - Beneficiary reach																							
T5.1 Identify potential users of the platform	x	x	x	x	x			▨	▨	▨	▨	▨	▨	▨	▨	▨	▨						
T5.2 Onboard first users	x		x	x	x													▨	▨	▨	▨	▨	▨

Project Expected Results

KPI

- Number of tools to facilitate and automate CRA compliance.
- Number of CRA essential requirements fully covered by tools.
- Number of CRA essential requirements partially covered by tools.
- Number of tools to simplify and automate CRA compliance documentation obligations.
- Number of awareness raising, dissemination and other stakeholder engagement activities.
- Number of workshops, training sessions, and events that facilitate interaction and CRA compliance among European SMEs.
- Number of CRA compliance use-cases and best-practices.
- Number of prospective companies which will benefit from tools developed by the project, of which SMEs.
- Number of prospective products and end-users benefiting from the tools.

Outcomes

- Tools to simplify and automate CRA compliance, with particular focus towards automated compliance tools that would ensure alignment with the CRA cybersecurity essential requirements.
- Tools to simplify and automate CRA compliance documentation obligations.

OSCRAT Consortium Partners

UNICIS

OVES ENTERPRISE

SENERSEC

Digital Innovation Hub
Trakia

PMF RESEARCH

Łukasiewicz
EMAG