SECURE

Cyber Resilience for SMEs

ANNEX 2 - CRA Scope & Eligible Activities, Services and Goods

Funded by the European Union

EU Funding Statement: Funded by the European Union under GA No 101190325. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre.
Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC disclaimer: The Project is supported by the European Cybersecurity Competence Center and its members

Table of Contents

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Introduction

This Annex to the Guidelines of the first SECURE Open Call aims to provide guidance on the eligibility requirements related to the CRA scope that Applicant Companies must meet, as well as on the activities, services, or goods for which co-funding may be requested.

- **The first chapter** outlines the scope of application of the CRA, with the objective of clarifying which types of companies may apply for funding. In particular, the core businesses of the companies must be assessed in relation to the types of products that fall within the CRA's scope.
- **The second chapter** provides a list of activities, services, and goods that may be eligible for co-funding. All listed activities may serve as inspiration for the drafting of Project Proposals and are intended to strengthen the Applicant Companies' level of compliance with the CRA.

When drafting Project Proposals using this document as a reference, it should be kept in mind that the CRA will be formally adopted by the European Union and its main obligations will be enforced by Member States, with the enforcement period completed by 2027. For this reason, and in the absence of more detailed regulatory provisions, the assessment of compliance with CRA-related eligibility requirements will be based on the Regulation itself and on the official guidelines currently available.

Given the current phase of CRA implementation, and with the intention of supporting as many companies as possible, all Proposals from mSMEs that could potentially fall within the CRA's scope will be considered eligible. This approach applies not only to companies that would currently fall within the CRA's scope, but also to those that, due to planned business or production developments, will fall under its scope in the near future.

Subcontracting

All activities listed in Chapter 2 may be implemented either by the applicant company's own staff or by a third-party provider selected by the applicant (e.g., consultants or service providers). If the activities are to be carried out by a provider/supplier, the related costs will be classified as subcontracting costs, which are considered eligible for funding under the present call.

The choice of provider must be documented by including information about the selected supplier in both *ANNEX 1.3 – Proposal Budget Template* and *ANNEX 1.1 – Proposal Template*.

Specific rules regarding subcontracting are described in *ANNEX 1.2 – Proposal Budget Guidelines*.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1. CRA SCOPE and CRA-related eligibility Requirements

1.1. *Introduction and preliminary remarks*

The Cyber Resilience Act (CRA), Regulation (EU) 2024/2847, introduces horizontal cybersecurity requirements for products with digital elements (PDEs) placed on the Union market. Only those companies whose activities and products potentially fall within the scope of the CRA are eligible to apply under this call.

It is important to underline that the CRA will become fully applicable on 11 December 2027, with certain obligations (such as the duty to report exploited vulnerabilities and cybersecurity incidents) entering into force on 11 September 2026. Until then, the assessment of whether a company or product is in scope must remain flexible and rely on current guidance provided by the European Commission and ENISA:

- European Commission – Cyber Resilience Act [1]
- ENISA – Cybersecurity for Products with Digital Elements[2]

This annex explains in detail the scope of the CRA, identifies the categories of products covered, clarifies the role of manufacturers, importers and distributors, and provides examples of how companies may be affected.

1.2. *Core Principles of the CRA*

At its core, Regulation (EU) 2024/2847 — the Cyber Resilience Act (CRA), establishes horizontal cybersecurity requirements for products with digital elements placed on the EU market. Its main aim is to ensure that digital products and services are[3]:

- secure by design, with cybersecurity embedded from the earliest stages of conception, development, and production;
- resilient to cyber threats, capable of resisting exploitation and adapting to emerging vulnerabilities; and
- capable to provide continuing protection throughout their life cycle, supported by secure update mechanisms and vulnerability handling processes.

The CRA addresses the growing risks associated with increased connectivity by making mandatory cybersecurity controls for a broad category of digital products, irrespective of where they are manufactured, as long as they are made available on the EU market.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R2847-20241120

[2]https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en https://www.enisa.europa.eu/topics/product-security-and-certification

[3] For more information and detailed clarification, please consult Chapter 5 of CRA101: Understanding CRA Obligations; and Chapters 3 and 5 of the CRA Methodological Compliance Assessment Framework.

By introducing the concept of security-by-design, the CRA marks a shift from reactive to preventive cybersecurity regulation. Rather than relying on voluntary measures or fragmented sectoral standards, the CRA establishes a common European framework where trust in digital products derives from mandatory, built-in security. In addition to the harmonisation of obligations across EU Member States (where it is directly applicable), this Regulation raises the bar globally, influencing also the practices of all non-EU manufacturers who wish to access the European market.

1.3. *Scope of application (Article 2 of CRA)*

According to Article 2, the CRA applies to all products with digital elements whose intended or reasonably foreseeable use involves a direct or indirect data connection, physical or logical, to a device or to a network.

1.3.1. Definition of Products with Digital Elements

A product with digital elements (PDE) is any software or hardware product, including remote data processing solutions, which has digital components and is capable of connectivity[4].

The scope also includes hardware or software components of PDEs when placed on the market separately.

1.3.2. Exclusions

Certain products already regulated by sector-specific legislation fall outside the CRA's scope:

- Medical devices (Regulation (EU) 2017/745) and in vitro diagnostic devices (Regulation (EU) 2017/746).
- Motor vehicles and related systems (Regulation (EU) 2019/2144).
- Civil aviation equipment (Regulation (EU) 2018/1139).
- Marine equipment (Directive 2014/90/EU).
- Identical spare parts for already certified components.
- Products developed exclusively for defence or national security purposes.
- Products specifically designed for processing classified information.

[4] See Article 3(1), Cyber Resilience Act (CRA)

1.4. *Product categories under the CRA*

Under the CRA, products with digital elements are classified into three main categories, designed to scale compliance efforts according to risk level[5]:

- **Default Products** – This encompasses the vast majority (around 90%) of products with digital elements. These products do not fall under higher-risk groups and can comply via self-assessment.
- **Important Products** (Annex III of CRA) – These are higher-risk items and further divided into:
  - Class I: Requires stricter checks, although often still via self-assessment if harmonized standards or common specifications exist.
  - Class II: Represents more critical items and mandates third-party conformity assessment.
- **Critical Products** (Annex IV of CRA) – These carry the highest cybersecurity risk and must undergo a European Common Criteria (EUCC) certification by a qualified conformity assessment body.

Category	Class	Brief Meaning	Compliance Procedure	Example Products
Default Products	–	Low-risk PDEs (~90% of total), general consumer or office devices	Compliance is demonstrated through internal control carried out by the manufacturer, leading to an EU declaration of conformity.	Standard printers, USB drives, office productivity tools, smart speakers, connected light bulbs, fitness trackers
Important Products	Class I	Higher-risk items requiring stricter checks, often still self-assessed if standards exist	For Class I items, manufacturers may rely on internal assessment provided harmonised standards or common specifications are followed.	Smart thermostats, connected webcams, home Wi-Fi extenders, smart locks, video doorbells, connected appliances (e.g., smart fridges)
	Class II	More critical items, requires third-party assessment	Class II items, by contrast, usually require the intervention of a notified body for third-party assessment.	Connected medical devices (non-regulated under MDR), industrial control systems, IoT gateways, building access control systems, payment terminals, cloud-connected surveillance systems
Critical Products	–	Highest cybersecurity risk, could severely affect safety, security, or privacy	These must undergo European Common Criteria (EUCC) certification, a rigorous process involving an accredited conformity assessment body.	Core telecom network equipment, 5G infrastructure, hardware security modules (HSMs), critical infrastructure management systems, AI-based cybersecurity defence platforms

[5] For more information and detailed clarification, please consult Chapter 5 of CRA101: Understanding CRA Obligations; and Chapters 3 and 5 of the CRA Methodological Compliance Assessment Framework.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.5. Economic operators under CRA Scope

The CRA establishes a clear distribution of obligations along the supply chain, ensuring that cybersecurity is addressed not only at the point of manufacture but also during importation, distribution, and product modification.

This chain of responsibility ensures that cybersecurity is not treated as a one-off requirement but as a continuous obligation binding every actor involved in the product lifecycle.

The table below illustrates specific examples for each operator, showing potential CRA-related implications.

Operator	CRA Article	Responsibilities Examples	Examples of hypothetical scenarios[6]
Manufacturer	Art. 13	• Design products securely (secure by design / secure by default) • Perform risk assessments • Prepare and retain technical documentation • Apply CE marking • Provide security updates and manage vulnerabilities • Notify exploited vulnerabilities and incidents within 24h	*A manufacturer of smart thermostats discovers a vulnerability. They must release a firmware update, inform customers, and report the incident to authorities within 24h.*
Importer[7]	Art. 19	• Place products on EU market only if compliant • Verify CE marking and conformity • Retain technical files for 10 years • Cooperate with authorities	*An importer of network firewalls must ensure CE marking and conformity before selling. If they rebrand the product or alter its software, they are considered the manufacturer under CRA.*
Distributor[8]	Art. 20	• Confirm CE marking and conformity before distribution • Avoid distributing risky products • Notify authorities of vulnerabilities/incidents	*A distributor of connected video doorbells detects a vulnerability leaking credentials. They must halt sales, notify authorities, and coordinate with the manufacturer. If they market the product under their own brand, they are considered the manufacturer.*
Open-source software stewards	Art. 24	• Ensure software is maintained securely • Provide information on vulnerabilities • Cooperate with authorities and stakeholders	*An open-source maintainer finds a vulnerability in a library used in IoT devices. They publish fixes and coordinate with users to mitigate the issue.*

[6] **DISCLAIMER**: In the absence of detailed legislative provisions on the transposition of the CRA, the examples provided below represent fictional yet realistic scenarios, based on a provisional interpretation of the Regulation. The products, contexts, and scenarios mentioned may ultimately fall outside the scope of the CRA or constitute only partially accurate representations, particularly following the formal transposition of the CRA.

[7] Art. 22: Importers become manufacturers if they place products on the market under their own name/brand or substantially modify them.

[8] Art. 22: Distributors become manufacturers if they place products under their own name/brand or substantially modify them.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.5.1. Authorized Representative (AR) – Art. 18

(Not an independent operator category in the same sense as manufacturers, importers, or distributors — instead, an entity appointed by a non-EU manufacturer.)

- Acts as EU contact point for manufacturers outside the EU.
- Holds technical documentation and the EU Declaration of Conformity.
- Responds to information requests from authorities.
- Cooperates with authorities and may transmit notifications if delegated.

Example: An EU-based AR for a non-EU IoT sensor producer provides full technical documentation during an audit or answers questions on security updates and vulnerability handling.

1.5.2. Substantial Modifications – Art. 22

Any operator (including importers, distributors, or third parties) who substantially modifies a product with digital elements in a way that affects compliance is legally considered a manufacturer and must meet all manufacturer obligations (documentation, CE marking, vulnerability management, incident reporting). This is not a separate operator category but a legal reclassification.

1.6. Product-Related examples of hypothetical scenarios[9]

The following are examples of potential implications of CRA application. They are conditional scenarios, illustrating what could happen rather than requirements. Each example highlights operational, regulatory, and supply chain considerations.

Smart Home Device Vulnerability *A widely sold smart thermostat could be discovered to allow unauthorized remote access to the home network. Manufacturers might need to issue an urgent firmware update, coordinate with distributors to halt shipments of affected units, and notify authorities. End users could experience temporary service disruption. This scenario shows how CRA obligations may trigger cross-actor coordination and operational responses.*	**Connected Security Camera Incident** *A networked indoor security camera might be found to transmit unencrypted video streams to third-party servers. Distributors could need to halt sales, importers might have to review technical documentation, and manufacturers could release a patch to encrypt the data. Authorities may require reporting of the vulnerability, illustrating the CRA's impact on consumer privacy and cybersecurity obligations.*
Industrial IoT Gateway Flaw *An IoT gateway used in smart buildings could be discovered to allow unauthorized access to connected sensors. Manufacturers may need to release a software update, distributors could halt deliveries of the affected batch, and importers may be asked to verify the updated compliance files. Building operators might need to apply patches, showing CRA's impact on industrial IoT and operational continuity.*	**Connected Office Printer Exploit** *A multifunction network printer might be found to have a flaw that allows attackers to access the office network via the device. The manufacturer might release a firmware update, while distributors ensure that affected units are held from sale until patched. Importers could be responsible for verifying the CE compliance of new shipments. This example illustrates CRA's role in ensuring cybersecurity even for low-risk office devices.*

[9] **DISCLAIMER**: see note n. 6

Smart Light Bulb Vulnerability *A brand of connected light bulbs could be discovered to be susceptible to remote takeover, potentially forming part of a botnet. Manufacturers might provide an over-the-air security update, distributors could notify retailers to stop selling vulnerable units, and importers may need to retain technical documentation for audit. End users would be guided to apply updates, showing CRA's implications for consumer IoT safety.*	**Cloud-Connected Video Doorbell Breach** *A cloud-connected video doorbell could leak access credentials due to insecure API design. The manufacturer might update firmware and cloud authentication methods, while importers and distributors coordinate compliance documentation and communication to users. Authorities could be notified if the vulnerability is actively exploited. This scenario highlights CRA's influence on software, firmware, and post-market surveillance.*

1.7. From CRA scope to CRA-related requirements of SECURE Project

Even though the CRA will become fully applicable only in December 2027, companies are strongly encouraged to begin aligning their processes with CRA requirements now. Anticipating obligations will not only ease the transition once the Regulation is fully enforceable but will also strengthen Applicants' market readiness and resilience in the short term.

The main purpose of the SECURE Project is to support SMEs in preparing for CRA compliance through funding activities and services that directly contribute to meeting CRA obligations. Verification of CRA relevance will form part of the evaluation process carried out by the designated SECURE partners. Applicants must demonstrate that their proposed activities are clearly linked to CRA obligations and that they fall within the scope of the Regulation.

2. Open Call CRA-related Fundable Activities, Services & Goods

The following list provides generic examples of fundable activities, goods, and services, intended to serve as a guide for Applicants in identifying the types of activities eligible to receive support. However, beyond these examples, additional services may also be proposed if they demonstrably and directly contribute to the achievement of CRA conformity.

Note for Applicants:

For further inspiration on fundable activities, Applicants are encouraged to consult the specific guidance published on SECURE web channels, including Understanding CRA Obligations – CRA 101, the CRA Methodological Compliance Assessment Framework, and the CRA Essential Cybersecurity Requirements (Annex I, Part I). These provide templates, recommendations, and suggestions on CRA compliance beyond the examples listed below.

Category 1: Accredited trusted third-party audit with the CRA certificate

IMPORTANT NOTE: This activity will not be eligible for funding during the first call, but it will only become eligible once - following the transposition of the CRA in the individual Member States of the Union - the mechanisms and standards for product certification have been identified.

An Accredited Trusted Third-Party Audit is a formal, independent conformity assessment conducted by an organisation accredited under applicable EU frameworks. Its purpose is to verify that the product satisfies the essential cybersecurity requirements set out in the Cyber Resilience Act (CRA), including security-by-design principles, vulnerability handling processes, and secure update mechanisms. This service includes a structured audit plan, in-depth review of documentation, functional and security testing, identification of non-conformities with corrective actions, and, upon successful closure, the issuance of a CRA-compliant certificate. Such certification is a tangible demonstration of compliance, essential for both market access and customer trust.

Category 2: CRA Cybersecurity Governance, Risk Management and Compliance Assessment – Module 1: CRA Conformity Gap Analysis

This CRA Conformity Gap Analysis systematically examines whether the supporting processes for the manufacturing or distribution of a CRA-product meet CRA requirements. It benchmarks current practices against mandated controls—such as vulnerability disclosure, logging, security updates, and documentation—and identifies any deficiencies. The outcome is a prioritised gap register, enabling the Applicant to clearly understand the specific technical and organisational measures needed to achieve full compliance.

Deliverable Examples	Description	KPIs examples
CRA Conformity Gap Analysis Report	*Document outlining gaps in current processes vs CRA requirements*	*Number of CRA controls evaluated*
Gap Analysis Register	*Spreadsheet or table listing identified deficiencies and criticality levels*	*Percentage of identified gaps documented in the Gap Register*
Compliance Checklist	*Document verifying adherence to key CRA controls: vulnerability disclosure, logging, updates, documentation*	*Number of high-priority gaps identified vs total gaps*
Executive Summary of Findings	*Presentation or PDF summarising major gaps and recommended actions*	*Completion rate of the compliance checklist*
Evidence Compilation Package	*Folder of supporting documents demonstrating current practices and identified gaps (resulting policies or procedures*	*No. of policies drafted*

Milestone Example:

- Completion of initial CRA controls assessment and gap identification
- Delivery of the prioritised Gap Register and compliance checklist
- Submission of the final CRA Conformity Gap Analysis Report with executive summary

Category 2: CRA Cybersecurity Governance, Risk Management and Compliance Assessment – Module 2: CRA Compliance Needs and Risk Analysis

This assessment evaluates compliance needs in relation to identified risks across the entire product lifecycle. It considers threat scenarios, likelihood and impact analysis, dependency on third-party components, and potential regulatory exposure. Risks are mapped to relevant CRA controls, ensuring that mitigation strategies are aligned with both security and legal obligations.

Deliverable Examples	Description	KPIs examples
CRA Risk Assessment Report	*Document mapping identified risks to CRA controls / Risk analysis models*	*Number of risks identified and classified (low/medium/high)*
Threat Scenario Analysis Document	*Report detailing potential threats, likelihood, and impact*	*Number of analysed threats and quantified impacts*
Third-Party Component Risk Register	*Spreadsheet listing dependencies and associated risks*	*Number of critical third-party components assessed*
Regulatory Exposure Assessment	*Document summarising potential non-compliance (NC) penalties and obligations*	*Number of NC / Regulation / Controls Analysed*
Risk Mitigation Recommendations Package	*Presentation or PDF outlining suggested corrective actions and priorities*	*Number of mitigation actions proposed*

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Milestone Example:

- Completion of threat scenario mapping and initial risk identification
- Delivery of the Risk Register and Regulatory Exposure Assessment
- Submission of the final CRA Compliance Needs and Risk Analysis Report

Category 2: CRA Cybersecurity Governance, Risk Management and Compliance Assessment – Module 3: CRA Remediation Plan

The CRA Remediation Plan is a structured, actionable roadmap to close identified compliance gaps. It defines remediation activities, assigns responsibilities, sets timelines, and details resource needs. The plan is aligned with the organisation's development cycles, ensuring that compliance improvements are embedded into regular product releases rather than handled as one-off interventions.

Deliverable Examples	Description	KPIs examples
CRA Remediation Plan Document	*Actionable roadmap detailing remediation activities, responsibilities, and timelines*	*Percentage of identified gaps with assigned remediation actions*
Resource Allocation Plan	*Spreadsheet or chart indicating assigned personnel, budget, and tools for each remediation task*	*Number of remediation tasks completed on schedule*
Remediation Activity Tracker	*Log or dashboard showing progress on corrective actions*	*Number of resources allocated versus planned*
Updated Gap Closure Register	*Document showing status of previously identified gaps*	*Reduction in number of critical non-compliances over time*
Evidence of Implemented Remediations	*Technical documents or material showing that the implementation of a remediation action has been achieved*	*No. of uploaded evidence assessing the implementation of the remediations*

Milestone Example:

- Approval of the initial Remediation Plan by Project stakeholders
- Completion of x% of remediation activities
- Full closure of identified compliance gaps and finalization of the Remediation Plan

Category 3: CRA requirements training

A targeted training programme that equips staff with a clear understanding of CRA obligations and essential cybersecurity requirements. Topics include secure design principles, documentation duties, conformity assessment pathways, post-market surveillance obligations, and vulnerability handling. The goal is to create shared awareness across all relevant teams, minimising errors and ensuring a unified compliance approach.

Deliverable Examples	Description	KPIs examples
Training Curriculum Document	*Detailed syllabus covering CRA obligations and cybersecurity requirements*	*Number of requirements covered*
Training Slides / Presentation Deck	*PowerPoint or PDF for training sessions*	*Number of documents shared with the attendees*
Attendance and Completion Records	*List of staff members who attended and completed the training / Recording of training session*	*Number of staff members trained* *Number of training sessions conducted*
Training Assessment Results	*Quiz or test results to measure understanding*	*Percentage of participants passing the training assessment* *Average score of participants in training assessments*
Training Feedback Report	*Summary of participants' feedback and improvement suggestions*	*Participant satisfaction rating*

Milestone Example:

- Completion of initial training session for all relevant teams
- 100% of staff passing the training assessment
- Delivery of final training report and feedback compilation

Category 4: CRA-related cybersecurity trainings

Practical, technical upskilling for developers, engineers, and security staff to align day-to-day operations with CRA requirements. Subjects may include secure coding practices, threat modelling techniques, handling open-source components securely, and remediation of vulnerabilities identified in assessments. Training is designed to have immediate operational impact.

For Deliverable Example see "CRA requirements Training Activity".

Category 5: Expertise support in the CRA conformity Project execution

Specialist advisory and hands-on Project execution support to steer the CRA compliance process. Experts provide technical guidance, review artefacts, coordinate remediation workstreams, and monitor progress. This activity is particularly valuable for SMEs lacking in-house CRA expertise, ensuring accuracy and efficiency throughout the Project.

Deliverable Examples	Description	KPIs examples
Technical Guidance Reports	*Documentation of advice provided on compliance measures*	*Number of compliance measures covered*
Reviewed Artefacts	*Updated policies, procedures, or technical documents*	*Number of policies drafted and/or implemented*

Workstream Coordination Logs	*Records of tasks, assignments, and progress*	*Percentage of Project artefacts reviewed and approved*
Progress Monitoring Reports	*Tracking compliance Milestones and gap closure*	*Number of compliance gaps addressed based on expert guidance*
Advisory Session Summaries	*Meeting notes detailing recommendations and next steps*	*Number of meetings* *Number of recommendations implemented*

Milestone Example:

- Completion of initial compliance review by experts
- Finalization of remediation workstream plans
- Submission of consolidated progress monitoring report

Category 6: Vulnerability tests

Regular vulnerability assessments of the product—covering software, firmware, and hardware components—to identify exploitable weaknesses. Assessments may include static and dynamic analysis, configuration reviews, and dependency checks. Early detection of vulnerabilities is essential to address them before they can be exploited, directly supporting CRA compliance.

Deliverable Examples	Description	KPIs examples
Vulnerability Assessment Reports & Remediation Plan	*Detailed documentation of detected vulnerabilities and suggested fixes*	*Number of vulnerabilities identified* *Number of conducted VA* *Number of systems/applications analysed* *Coverage percentage of systems/components tested*
Static and Dynamic Analysis Logs	*Records from automated code scans and runtime tests*	
Configuration Review Reports	*Assessment of system and device configurations*	*Severity distribution of detected vulnerabilities*
Dependency Check Reports	*Analysis of third-party libraries or components*	*Number of libraries tested*
Patches & Fixes	*Implementation of patches and fixes for identified vulnerabilities*	*Number of vulnerabilities remediated*

Milestone Example:

- Completion of initial vulnerability assessment
- Implementation of remediation actions for critical vulnerabilities
- Approval of final vulnerability assessment report by compliance team

Category 7: Laboratory tests

Controlled lab-based testing to verify that a product's security features—such as encryption, authentication, and access control—operate as intended under reproducible conditions. These tests provide authoritative evidence that the product meets essential CRA requirements.

Deliverable Examples	Description	KPIs examples
Technical Guidance Reports	*Documentation of advice provided on compliance measures*	*Number of compliance measures covered*
Reviewed Artefacts	*Updated policies, procedures, or technical documents*	*Number of policies drafted and/or implemented*
Workstream Coordination Logs	*Records of tasks, assignments, and progress*	*Percentage of Project artefacts reviewed and approved*
Progress Monitoring Reports	*Tracking compliance Milestones and gap closure*	*Number of compliance gaps addressed based on expert guidance*
Advisory Session Summaries	*Meeting notes detailing recommendations and next steps*	*Number of meetings* *Number of recommendations implemented*

Milestone Example:

- Completion of initial laboratory testing for all targeted security features
- Verification of encryption, authentication, and access control functionality
- Review and approval of technical guidance and artefacts by stakeholders

Category 8: Penetration tests

Authorised simulated cyberattacks performed by experienced testers to assess real-world exploitability of vulnerabilities. Penetration testing under CRA covers multiple attack surfaces—firmware, APIs, cloud interfaces, embedded systems—and demonstrates both compliance and product resilience.

Deliverable Examples	Description	KPIs examples
Penetration Test Report & Remediation Plan	*Documented exploits and suggested fixes*	*Number of successful exploits* *Systems tested* *Attack surface coverage*
Proof-of-Concept Exploits	*Demonstrations of attacks*	*Number of PoCs* *Severity of vulnerabilities*
Configuration & Dependency Review	*Assessment of system and third-party risks*	*Number of misconfigurations* *Libraries/components tested*
Remediation Verification	*Validation of fixes*	*Number of vulnerabilities mitigated*

Milestone Example:

- Completion of initial penetration test
- Critical exploits demonstrated
- Mitigations applied and verified

Category 9: CRA third-party assessment service

IMPORTANT NOTE: This activity will not be eligible for funding during the first call, but it will only become eligible once - following the transposition of the CRA in the individual Member States of the Union - the mechanisms and standards for product certification have been identified.

An independent assessment performed by an authorised organisation to evaluate CRA conformity. This service provides unbiased verification of compliance and is particularly critical for high-risk product categories where third-party assessment is mandated by the CRA.

Category 10: CRA self-assessment tool

A structured self-evaluation tool—such as a checklist or software platform — that guides organisations through CRA requirements. It facilitates early detection of compliance gaps, supporting proactive remediation and reducing reliance on reactive fixes.

Deliverable Examples	Description	KPIs examples
Self-Assessment Reports	*Completed evaluations showing compliance status*	*Number of assessments completed* *Compliance gaps identified* *Coverage of CRA requirements*
Checklist / Tool Outputs	*Structured guidance and automated checks*	*Number of items evaluated* *Percentage of requirements assessed*
Remediation Plan	*Actions for addressing detected gaps*	*Number of gaps addressed* *Time to implement corrective actions*
Progress Tracking Dashboard	*Visualization of compliance improvements*	*Improvement rate over time* *Number of issues closed*

Milestone Example:

- Completion of initial self-assessment
- Identification of compliance gaps
- Implementation of remediation actions

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Category 11: Software Development – Security by Design for CRA Products

Integration of security into the Software Development Lifecycle (SDLC) in alignment with CRA principles. This includes threat modelling, secure coding standards, software bill of materials (SBOM) management, and security testing embedded in CI/CD pipelines.

Deliverable Examples	Description	KPIs examples
Secure Design & Threat Models	*Documentation of security requirements and threat scenarios*	*Number of threats identified* *Coverage of critical components*
Secure Code & SBOM	*Code developed following secure coding standards and SBOM maintained*	*Number of code issues detected* *Percentage of components with SBOM*
Security Testing Reports	*Results from ci/cd-integrated static, dynamic, and dependency tests*	*Number of vulnerabilities detected* *Test coverage percentage*
Remediation & Verification	*Fixes applied and verified in development pipeline*	*Number of issues resolved* *Time to remediation*

Milestone Example:

- Completion of threat modelling
- Integration of secure coding practices and SBOM
- Execution of automated security tests

Category 12: Business Continuity, Incident and Response Planning for CRA Products and Processes

Development of operational frameworks for incident detection, response, and recovery that meet CRA expectations. This includes urgent maintenance procedures, secure update rollouts, and customer communication protocols in the event of incidents.

Deliverable Examples	Description	KPIs examples
Incident Response Plan	*Documented procedures for detecting, responding to and recovering from incidents*	*Number of incidents detected* *Mean time to respond (MTTR)* *Coverage of critical processes*
Business Continuity Plan	*Framework for maintaining essential operations during disruptions*	*Recovery time objectives (RTO)* *Recovery point objectives (RPO)* *Plan completeness percentage*
Test & Simulation Reports	*Results from drills, simulations and scenario exercises*	*Number of tests conducted* *Response effectiveness* *Gap closure rate*

Communication Protocols	*Defined procedures for notifying stakeholders and customers during incidents*	*Number of communications executed on time* *Stakeholder satisfaction*

Milestone Example:

- Completion of initial incident and business continuity plans
- Execution of first simulation/drill
- Implementation of corrective actions from tests

Category 13: Supply Chain Risk & Security Assessment

Comprehensive evaluation of third-party suppliers and components to ensure they meet CRA security requirements. Activities include supplier audits, contractual security provisions, and SBOM-driven risk assessment to minimise supply chain vulnerabilities.

Deliverable Examples	Description	KPIs examples
Supplier Security Assessment Reports	*Evaluation of third-party suppliers against CRA requirements*	*Number of suppliers assessed* *Severity of risks identified* *Coverage of critical suppliers*
Audit & Verification Reports	*Evidence from on-site or remote supplier audits*	*Number of audits conducted* *Compliance gaps detected*
SBOM-Based Risk Analysis	*Assessment of third-party components using software bill of materials*	*Number of components analysed* *Vulnerabilities identified*
Remediation & Mitigation Plan	*Actions to address supply chain risks*	*Number of risks mitigated* *Time to implement corrective actions*

Milestone Example:

- Completion of initial supplier assessments
- Execution of supplier audits
- Identification and mitigation of critical supply chain risks

Category 14: Data Protection & Privacy Compliance

Alignment of product design and operation with data protection laws, including GDPR, in harmony with CRA obligations. This ensures that security and privacy are addressed jointly, covering data minimisation, secure storage, and breach handling.

Deliverable Examples	Description	KPIs examples

Data Protection Impact Assessment (DPIA)	*Evaluation of data processing activities against CRA and privacy requirements*	*Number of DPIAs completed* *Number of compliance gaps identified*
Privacy & Security Controls Implementation	*Integration of data minimisation, encryption, and access controls*	*Percentage of systems with controls implemented* *Number of control failures detected*
Breach Response & Reporting Plan	*Procedures for detecting, reporting, and mitigating data breaches*	*Mean time to detect/respond (MTTD/MTTR)* *Number of breaches reported on time*
Compliance Verification Reports	*Documentation of audits and reviews confirming privacy compliance*	*Number of audits conducted* *Number of issues remediate*

Milestone Example:

- Completion of initial DPIA
- Implementation of privacy and security controls
- Execution of breach response exercises

Category 15: CRA Regulatory Obligations and Documentation Support

IMPORTANT NOTE: This activity will not be eligible for funding during the first call, but it will only become eligible once - following the transposition of the CRA in the individual Member States of the Union - the mechanisms and standards for product certification have been identified.

Support in preparing and maintaining CRA-mandated technical documentation and regulatory records, such as declarations of conformity, post-market surveillance plans, and vulnerability disclosure policies.

Category 16: Monitoring, protection and prevention services and tools

Deployment of tools and services for continuous monitoring, proactive threat prevention, and incident detection. Examples include intrusion detection systems, malware scanning, access control, privilege management, and encryption solutions.

Deliverable Examples	Description	KPIs examples
Monitoring & Detection Tools	Deployment of IDS malware scanners, and logging systems	Number of systems monitored Number of threats detected
Access & Privilege Management	Implementation of controls to manage user access and privileges	Number of privileged accounts managed Access violations detected
Encryption & Data Protection	Deployment of encryption and secure storage solutions	Percentage of data encrypted Number of data protection incidents

Threat Prevention & Response Reports	Reports on detected threats, prevention measures, and mitigation actions	Number of threats prevented Mean time to respond (MTTR)

Milestone Example:

- Deployment of monitoring and protection tools
- Implementation of access and privilege controls
- Execution of threat detection and prevention procedures

Goods and Licensing

Applicants may also purchase goods or technologies where such acquisitions are necessary to complete one of the eligible activities mentioned above, or where they are instrumental to the successful implementation of the Project or the achievement of CRA compliance objectives.

In particular, eligible purchases may include cybersecurity and digital resilience technologies aimed at protecting information systems, production environments, or the products themselves.

Please note that the costs of goods and licenses will be covered only for the period of use within the 180-day Project implementation timeframe.

Examples may include, but are not limited to[10]:

- Network security tools, such as firewalls, intrusion detection and prevention systems (IDS/IPS), and next generation gateways;
- Data protection technologies, including encryption software, secure key management systems, and data loss prevention (DLP) solutions;
- Endpoint and device security solutions, such as antivirus, endpoint detection and response (EDR), Extended;
- Detection and Response (XDR) or mobile device management (MDM);
- Vulnerability and compliance management tools, including penetration testing software, automated patch management systems, and vulnerability scanners;
- Secure development and monitoring environments, such as code analysis platforms, continuous security monitoring tools, and logging/alerting systems (e.g., SIEM);
- Production environment protection, e.g., industrial firewalls, intrusion detection for operational technology (OT), and access control devices;
- Secure cloud services and container security tools, including cloud workload protection platforms (CWPP) and container scanning solutions;
- Identity and access management (IAM) solutions, multi-factor authentication (MFA) systems, and privileged access management (PAM) tools;

[10] For more examples and recommended tools that may assist in your CRA compliance, please consult the CRA Methodological Compliance Assessment Framework.

- Software Bill of Materials (SBOM) management tools and dependency scanning solutions for supply chain security;
- Incident detection, response, and recovery platforms, including automated alerting and orchestration tools;
- Secure update and patch management solutions for embedded systems or IoT devices.

IMPORTANT NOTE: The purchase of goods will be carefully evaluated by the Evaluation Committee to verify to verify that both the declared costs and the goods to be acquired are consistent with the project proposal. The examples provided above do not necessarily represent items that will be accepted during the Proposal submission. Their eligibility will depend on the implementation context and on their relevance within the proposed Project.