SECURE
Cyber Resilience for SMEs

CRA Methodological Compliance Assessment Framework

20/10/2025

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

DISCLAIMER

This document is part of Deliverable D4.1 'Guidelines and Materials for SMEs CRA Compliance' of the SECURE Project.

First author: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Second author: *Centre for Cybersecurity Belgium (CCB)*

Table of contents

List of Tables and Figures

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Abbreviations

AES – Advanced Encryption Standard

API - Application Programming Interface

CI/CD – Continuous Integration and Continuous Delivery/Deployment

CIS – Centre for Internet Security

CRA – Cyber Resilience Act

CSIRT – Computer Security Incident Response Team

CVD – Coordinated Vulnerability Disclosure

CVE – Common Vulnerabilities and Exposures

CVSS – Common Vulnerability Scoring System

CWS – Common Weakness Enumeration

DDoS – Distributed Denial of Service

DMS – Document Management System

DPIA - Data Protection Impact Assessment

ECDSA - Elliptic Curve Digital Signature Algorithm

ENISA – European Union Agency for Cybersecurity

ETSI – European Technical Standard Institute

EU – European Union

EU DoC – European Union Declaration of Conformity

EUCS – EU Cloud Security

FTP – File Transfer Protocol

GDPR – General Data Protection Regulation

IDS – Intrusion Detection System

IEC – International Electrotechnical Commission

IoT – Internet of Things

IPS – Intrusion Prevention System

ISO – International Standards Organisation

MFA – Multi-Factor Authentication

NB – Notified Body

NIST – National Institute of Standards and Technology (United States)

NIST NVD – NIST National Vulnerability Database

OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation

OTA – Over The Air

OWASP – Open Worldwide Application Security Project

OWASP ESAPI – OWASP Enterprise Security API

OWASP SAMM – OWASP Software Assurance Maturity Model

OWASP ZAP – OWASP Zed Attack Proxy

PASTA – Process for Attack Simulation and Threat Analysis

PDE – Product with Digital Elements

PSIRT – Product Security Incident Response Team

RBAC - Role-Based Access Control

SBOM – Software Bill of Materials

SDLC – Secure Development Life Cycle

SIEM – Security Information and Event Management

SME – Small and Medium Enterprise

SNMP – Simple Network Management Protocol

SPDX – System Package Data Exchange

SQL – Structured Query Language

SSL – Secure Sockets Layer

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

TLS – Transport Layer Security

UPnP – Universal Plug and Play

VPN – Virtual Private Network

XSS – Cross-site Scripting

Introduction

The European Union's **Cyber Resilience Act (CRA)**, Regulation (EU) 2024/2847, establishes a comprehensive framework to ensure that products with digital elements (PDEs) are secure throughout their lifecycle, from design to end-of-life. To **assist Small and Medium Enterprises (SMEs) in evaluating and improving their CRA compliance status**, this document provides a methodological compliance self-assessment framework. It is part of the materials provided by the **SECURE Project**[1], aimed at supporting SMEs with the implementation of the CRA. Through an extensively detailed framework, **five key criteria** are expanded on: (1) Essential Cybersecurity Requirements Compliance, (2) Certification of Products with Digital Elements, (3) Classification of Products as Class I or Class II and Corresponding Actions, (4) Technical Documentation Completeness, and (5) Overall Conformity Assessment Procedures. Each section is enriched with in-depth guidance, practical examples, case studies, checklists, references to templates, tools, and standards, ensuring SMEs can effectively navigate CRA obligations with actionable strategies tailored to their resource constraints. However, they all remain of a **suggestive nature**, offering recommendations based on recognised approaches and best practices to support SMEs in their compliance trajectory. References to existing tools and frameworks are to be treated as illustrative. This guideline is subject to updates as the CRA legislative framework further develops.

[1] The 'Strengthening EU SMEs Cyber Resilience' (SECURE) project offers financial support and guidance for SMEs to comply with the CRA.

CRA Methodological Compliance Assessment Framework

1. Essential Cybersecurity Requirements Compliance

The **Essential Cybersecurity Requirements Compliance** criterion is the cornerstone of CRA compliance, ensuring that products with digital elements meet stringent cybersecurity standards to be placed on the EU market. Annex I of the CRA specifies 13 **Product Cybersecurity Requirements** and 8 **Vulnerability Handling Requirements**, totalling 21 essential requirements. This section provides an exhaustive methodology for SMEs to assess compliance, document evidence, identify gaps, and develop remediation plans. It includes detailed explanations, practical tools, case studies, templates, and step-by-step guidance to ensure thorough evaluation and compliance.

1.1. Product Cybersecurity Requirements

The product cybersecurity requirements mandate that products are designed and developed with security as a core principle ("secure by design and by default"). These requirements ensure that products are free from known exploitable vulnerabilities, have secure default configurations, support timely security updates, and protect data confidentiality, integrity, and availability. Below is a comprehensive exploration of the requirements[2], with detailed guidance, examples, tools, and methodologies.

1.1.1. No Known Exploitable Vulnerabilities

Manufacturers must ensure products are free from known exploitable vulnerabilities at release, requiring rigorous pre-release testing, including vulnerability scans, penetration testing, and code reviews. SMEs, often resource-constrained, can leverage cost-effective security testing and scanning tools (e.g., a web-application dynamic scanner, a network vulnerability scanner, a static application security testing tool, and a container image scanner)to identify issues. For example, a smart lock manufacturer should test for Bluetooth vulnerabilities, such as weak pairing protocols or replay attacks, and document remediation in a vulnerability management log. Testing should align with standards like **OWASP Top 10** or **CWE/SANS Top 25** to cover common vulnerabilities.

[2] Some of the CRA Annex I overlapping requirements are grouped together in this guideline, resulting in a list of eight concrete obligations.

Detailed Guidance:

- **Vulnerability Scanning**: Use OpenVAS or Nessus to scan for CVEs, scheduling scans biweekly during development. SMEs can access free tiers of tools like Trivy for container-based applications.
- **Penetration Testing**: Conduct manual or automated tests using tools like Metasploit or engage third-party providers for quarterly assessments. Focus on high-risk areas like authentication or network interfaces.
- **Code Reviews**: Use SonarQube to detect code-level vulnerabilities, such as SQL injection or cross-site scripting (XSS). Implement peer reviews for critical components.
- **Documentation**: Maintain a vulnerability management log with columns for CVE ID, CVSS score, affected component, remediation action, and status. Use tools like Jira or Trello for tracking.
- **Remediation Plan**: For unpatched vulnerabilities, prioritise based on CVSS scores (e.g., >7.0 as critical) and set remediation timelines (e.g., 30 days for critical issues).

Case Study: An SME developing a smart thermostat conducts a vulnerability scan using Nessus, identifying a weak encryption protocol (TLS 1.1). The SME upgrades to TLS 1.3, tests the fix with OWASP ZAP, and documents the process in a log, including CVSS scores and test reports. The self-assessment confirms no known vulnerabilities remain, supported by a penetration test report from a third-party provider.

Table 1:
Template Vulnerability Management Log

CVE ID	CVSS Score	Component	Description	Remediation Action	Status	Date Resolved
CVE-2025-1234	8.5	TLS 1.1	Weak encryption	Upgrade to TLS 1.3	Resolved	2025-06-15

1.1.2. Secure Default Configurations

Products must ship with hardened default settings to minimise risks, such as disabling unnecessary services, using strong passwords, and closing open ports. SMEs should align with **ETSI EN 303 645**, which provides IoT-specific guidelines, or **CIS Benchmarks** for specific technologies (e.g., Linux, Docker). For instance, a smart home camera should disable remote access by default, require unique passwords, and close unused ports like Telnet.

Detailed Guidance:

- **Configuration Review**: Develop a checklist based on ETSI EN 303 645, verifying settings like disabled debug modes, no default credentials, and closed ports. Use tools that do system hardening checks.
- **Port Scanning**: Use **Nmap** to identify open ports and services, ensuring only necessary ones are active. For example, disable FTP if not required.
- **Password Policies**: Implement strong default passwords or force users to set them during setup. Use password strength checkers.
- **Documentation**: Include configuration settings in the technical file, referencing standards like CIS Benchmarks. Document deviations and justifications.
- **User Guidance**: Provide setup instructions in user manuals, explaining how to maintain secure configurations (e.g., disabling guest Wi-Fi).

Case Study: An SME producing a Wi-Fi router ensures default settings disable UPnP and Telnet, using Nmap to verify closed ports. The self-assessment checklist confirms compliance with ETSI EN 303 645 Clause 5.1, supported by a configuration report and user manual instructions.

Table 2:
Template Configuration Checklist

Setting	Requirement	Status	Evidence	Notes
UPnP	Disabled	Compliant	Nmap scan report	Verified 2025-06-10

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.3. Prompt Security Updates

Products must support automatic security updates with user opt-out options. SMEs can use **over-the-air (OTA)** update mechanisms via platforms like **Mender.io, AWS IoT Device Management**, or **Balena**. Updates should be signed and verified using tools like **OpenSSL** to prevent tampering. For example, a wearable device manufacturer should ensure firmware updates address vulnerabilities within 30 days of discovery, with clear user notifications.

Detailed Guidance:

- **Update Infrastructure**: Set up an OTA update server or use cloud-based solutions. Ensure updates are signed with RSA-2048 or ECDSA.
- **Testing Updates**: Verify updates install without disrupting functionality, using test environments like **Docker**. Conduct regression testing to ensure compatibility.
- **User Notification**: Use email, in-app notifications, or LED indicators to inform users of updates. Provide opt-out instructions in user manuals.
- **Documentation**: Include update frequency, signing mechanisms, and user notification procedures in the technical file. Log update history with timestamps and CVEs addressed.
- **Compliance Metrics**: Track update deployment time (e.g., <30 days for critical patches) and user adoption rates.

Case Study: A smart speaker SME uses Mender.io to push signed firmware updates, addressing a CVE within 25 days. The self-assessment documents the OTA process, user notification via email, and regression test results, ensuring compliance with CRA requirements.

Table 3:
Template Update Log

Update ID	CVE Addressed	Release Date	Deployment Time	User Notification	Status
V2.1.3	CVE 2025-5678	2025-07-01	25 days	Email sent 2025-06-30	Deployed

1.1.4. Protection Against Unauthorised Access

Strong authentication mechanisms, such as **multi-factor authentication (MFA)**, **OAuth 2.0**, or **OpenID Connect**, are essential to prevent unauthorised access. SMEs can use **JSON Web Tokens (JWT)** for API security and **role-based access control (RBAC)** to limit permissions. Tools like **Burp Suite** or **Postman** can simulate attacks to test access controls. For example, a cloud-connected IoT device should require MFA for user accounts and use JWT for API endpoints.

Detailed Guidance:

- **Implement Authentication**: Use MFA libraries like **Auth0** or **Okta** for user accounts. Implement JWT for APIs, following RFC 7519.
- **Test Access Controls**: Conduct penetration tests with Burp Suite to simulate brute-force or session hijacking attacks. Use tools like **Wireshark** to monitor network traffic.
- **Document Policies**: Include authentication and access control policies in the technical file, detailing protocols (e.g., OAuth 2.0) and RBAC configurations.
- **Monitor Access**: Enable logging of access attempts using **Syslog** or **ELK Stack**, with alerts for suspicious activity (e.g., multiple failed logins).
- **Regular Audits**: Schedule quarterly audits of access controls, using tools like **HashiCorp Vault** for credential management.

Case Study: An SME developing a smart doorbell implements MFA using Auth0 and tests it with Burp Suite, identifying and fixing a session management flaw. The self-assessment includes authentication policies, test reports, and log configurations.

Table 4:
Template Access Control Policy

Component	Authentication	Access Control	Testing Method	Evidence	Status
User Login	MFA (Auth0)	RBAC (Admin/User)	Burp Suite	Test report 2025-06-20	Compliant

1.1.5. Data Confidentiality, Integrity, and Availability

Encryption is critical for protecting data. SMEs should implement **AES-256** for data at rest and **TLS 1.3** for data in transit, aligning with **NIST SP 800-52**. Input validation should prevent injection attacks, using libraries like **OWASP ESAPI**. For example, a health monitoring device must encrypt patient data to comply with GDPR and CRA, ensuring confidentiality and integrity.

Detailed Guidance:

- **Select Encryption Standards**: Use AES-256 for storage and TLS 1.3 for communication. Implement key management with **AWS KMS** or **HashiCorp Vault**.
- **Test Encryption**: Conduct penetration tests with Metasploit to verify data protection. Use tools like **SSL Labs** to assess TLS configurations.
- **Validate Inputs**: Implement input validation using ESAPI or similar libraries to prevent SQL injection or XSS.
- **Document Encryption**: Include encryption protocols, key management policies, and test results in the technical file.
- **Monitor Availability**: Use monitoring tools like **Nagios** to ensure system uptime and resilience against DDoS attacks.

Case Study: A medical device SME encrypts patient data with AES-256 and TLS 1.3, tests with Metasploit, and documents compliance in the technical file. Input validation prevents SQL injection, verified by OWASP ZAP scans.

Table 5:
Template Encryption Compliance

Data Type	Encryption	Key Management	Testing Method	Evidence	Status
Patient Data	AES-256	AWS KMS	Metasploit	Test report 2025-06-25	Compliant

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1.6. Data Minimisation and Attack Surface Reduction

Products should collect only necessary data and minimise open interfaces. SMEs can use **Nmap** to scan for open ports and **OWASP Dependency-Check** to identify unused dependencies. A **Data Protection Impact Assessment (DPIA)**, aligned with GDPR, should justify data collection. For example, a fitness tracker should limit data to heart rate and steps, disabling unused Bluetooth services.

Detailed Guidance:

- **Map Data Flows**: Conduct a DPIA to document data collection, processing, and storage. Use tools like **OneTrust** for DPIA automation.
- **Minimise Interfaces**: Use Nmap to identify and close unnecessary ports or APIs. Disable unused protocols like SNMP or FTP.
- **Remove Dependencies**: Use Dependency-Check to identify and remove unused libraries.
- **Document Minimisation**: Include DPIA results and interface configurations in the technical file.
- **Regular Reviews**: Schedule quarterly DPIA updates to reflect product changes.

Case Study: A fitness tracker SME conducts a DPIA, limits data collection to essential metrics, and disables unused Bluetooth services. Nmap scans confirm a minimal attack surface, documented in the self-assessment.

Table 6:
Template DPIA Summary

Data Type	Purpose	Necessity	Minimisation Action	Evidence	Status
Heart Rate	Health Monitoring	Essential	Disabled location tracking	DPIA report 2025-06-30	Compliant

1.1.7. Incident Mitigation and Logging

Products must include mechanisms to limit damage from incidents, such as rate-limiting or intrusion detection, and enable secure logging. SMEs can use tools for logging, ensuring tamper-proof storage. For example, a network router should log unauthorised access attempts and implement rate-limiting to prevent brute-force attacks.

Detailed Guidance:

- **Implement Mitigation**: Use rate-limiting (e.g., via **NGINX**) and intrusion detection systems like Snort.
- **Enable Logging**: Configure Syslog or ELK Stack for secure, encrypted logging. Set retention policies (e.g., 6 months).
- **Test Mitigation**: Simulate attacks with tools like **hping3** to verify rate-limiting and IDS effectiveness.
- **Document Logs**: Include log formats, retention policies, and test results in the technical file.
- **Review Logs**: Schedule monthly log reviews to identify anomalies, using tools like **Splunk** for analysis.

Case Study: A router SME implements rate-limiting with NGINX and logs access attempts with ELK Stack. Penetration tests with hping3 confirm mitigation, documented in the self-assessment.

Table 7:
Template Logging Configuration

Event Type	Log Format	Storage	Retention	Testing Method	Evidence	Status
Access Attempts	Syslog	Encrypted	6 months	hping3	Test report 2025-07-01	Compliant

1.1.8. User Data Deletion

Products must allow users to securely delete personal data, using cryptographic wiping techniques. For example, a smart speaker should offer a factory reset option that overwrites user data with tools like **a cryptographic library for secure wiping**. SMEs should verify deletion effectiveness with forensic tools.

Detailed Guidance:

- **Implement Deletion**: Provide a secure reset option, using cryptographic wiping (e.g., OpenSSL s_random).
- **Test Deletion**: Use forensic tools to verify data is unrecoverable.
- **Document Process**: Include deletion instructions and test results in the technical file.
- **User Guidance**: Provide clear instructions in user manuals, with online support for troubleshooting.
- **Regular Testing**: Schedule annual tests to ensure deletion mechanisms remain effective.

Case Study: A smart speaker SME implements a factory reset with cryptographic wiping, tested with Autopsy. The self-assessment includes user manual instructions and test reports.

Table 8:
Template Data Deletion Verification

Component	Deletion Method	Testing Tool	Evidence	Status
User Data	Cryptographic Wipe	Autopsy	Test report 2025-07-05	Compliant

1.2. Vulnerability Handling Requirements

The 8 vulnerability handling requirements ensure ongoing security management post-release, requiring processes for identifying, remediating, and disclosing vulnerabilities. Below is a detailed exploration of the requirements[3].

[3] As stated above, to avoid overlap, some requirements have been regrouped, resulting in a list six obligations.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.2.1. Software Bill of Materials (SBOM)

Manufacturers must maintain a machine-readable SBOM in formats like **CycloneDX** or **SPDX**. Tools like **Snyk**, **Dependabot**, or **Trivy** can automate SBOM generation. For example, a web application SME uses Dependabot to track dependencies and generate an SBOM, ensuring transparency for third-party components.

Detailed Guidance:

- **Generate SBOM**: Use Snyk or Trivy to create an SBOM, including version numbers and licenses.
- **Update SBOM**: Schedule monthly updates to reflect new components or patches.
- **Verify Components**: Check for vulnerabilities using NIST's NVD or Snyk's database.
- **Document SBOM**: Include the SBOM in the technical file, with a changelog for updates.
- **Integrate with CI/CD**: Use tools like **GitHub Actions** to automate SBOM generation in development pipelines.

Case Study: A cloud service SME generates an SBOM with CycloneDX, identifying a vulnerable library (Log4j). The SME patches the library, updates the SBOM, and documents the process in the self-assessment.

Table 9:
Template SBOM Summary

Component	Version	License	Vulnerability	Action	Status
Log4j	2.16.0	Apache 2.0	CVE-2021-44228	Patched to 2.17.1	Resolved

1.2.2. Timely Vulnerability Remediation

Vulnerabilities must be addressed without undue delay, prioritising critical issues based on **CVSS scores**. SMEs should release patches within 30 days for critical vulnerabilities and 60 days for others. For example, a smart camera SME patches a CVE within 25 days, notifying users via email.

Detailed Guidance:

- **Monitor Vulnerabilities**: Use Snyk, NIST’s NVD, or **VulnDB** to track CVEs.
- **Prioritise Patches**: Use CVSS scores to prioritise (e.g., >7.0 as critical, 4.0-6.9 as medium).
- **Test Patches**: Conduct regression testing in a sandbox environment to ensure stability.
- **Notify Users**: Use email, in-app notifications, or website advisories to inform users.
- **Document Remediation**: Include patch timelines, test results, and user notifications in the technical file.

Case Study: A smart lock SME identifies a critical CVE (CVSS 8.8) and releases a patch within 20 days, documenting the process and user notification in the self-assessment.

Table 10:
Template Vulnerability Remediation Log

CVE ID	CVSS Score	Component	Patch Date	Notification Method	Status
CVE-2025-5678	8.8	Firmware	2025-07-01	Email	Resolved

1.2.3. Regular Security Testing

Periodic testing, including penetration tests, vulnerability scans, and code reviews, is required. SMEs can use **OpenVAS**, **Nessus**, or third-party providers for cost-effective audits, scheduling quarterly scans and annual penetration tests.

Detailed Guidance:

- **Schedule Tests**: Plan quarterly vulnerability scans and annual penetration tests, aligning with **ISO 27001 Annex A.12.6.1**.
- **Use Tools**: Employ OpenVAS for scans, Burp Suite for web apps, or Metasploit for penetration testing.
- **Document Results**: Include test reports, findings, and remediation plans in the technical file.

- **Remediate Findings**: Prioritise issues based on severity and set remediation timelines.
- **Automate Testing**: Integrate tools like **Snyk** into CI/CD pipelines for continuous scanning.

Case Study: A smart home device SME conducts quarterly OpenVAS scans and an annual penetration test with a third-party provider, documenting results and remediation plans in the self-assessment.

Table 11:
Template Security Testing Schedule

Test Type	Frequency	Tool	Last Conducted	Findings	Remediation Status
Vulnerability Scan	Quarterly	OpenVAS	2025-06-30	2 CVEs	Resolved

1.2.4. Transparency in Vulnerability Disclosure

Manufacturers must publicly disclose vulnerability details and remedial updates once patches are available. SMEs should publish security advisories on their website detailing severity, impact, affected versions, mitigations/workarounds, and timelines, in line with recognised vulnerability-disclosure standards and good practices (e.g., ISO/IEC 29147 and ISO/IEC 30111, ENISA CVD guidance, FIRST multiparty coordination guidance, or an equivalent internal policy that maps to these).

Detailed Guidance:

- **Create Disclosure Template**: Develop a standard format for advisories, including CVE ID, CVSS score, impact, and patch details.
- **Publish Advisories**: Post on the company website, blog, or security portal.
- **Notify Users**: Use email, in-app notifications, or social media to inform users.
- **Document Disclosures**: Include a link or DMS path to your public advisory archive, the internal change log for the advisory text, and proof of user notifications (lists, timestamps, and channels).

- **Engage** Coordinators: Where appropriate, share advisories with relevant national CSIRTs/PSIRTs or vulnerability-coordination communities and archives to support broad awareness (use neutral channels; no specific brand is required).
- **State Your Basis:** In your public policy, name the guideline you align to (e.g., ISO/IEC 29147 and ISO/IEC 30111 or ENISA CVD good practice) and note that functionally equivalent processes are accepted. Keep the policy version/date and review it annually.

Case Study: A smart TV SME publishes a security advisory for a CVE, detailing the patch and impact. The self-assessment includes the advisory and user notification records.

Table 12:
Template Security Advisory

CVE ID	CVSS Score	Impact	Patch Details	Publication Date	Notification Method
CVE-2025-1234	7.5	Data Breach	Firmware v2.1.3	2025-07-01	Website, Email

Other columns can be added such as Affected Versions/Builds; Mitigations/Workarounds (if patch not yet available); Disclosure Timeline (report received - acknowledged - patched - published); Acknowledgements (researcher/CSIRT, if applicable).

1.2.5. Coordinated Vulnerability Disclosure (CVD) Policy

SMEs must provide a clear channel for reporting vulnerabilities, such as a dedicated email or web portal. Platforms like HackerOne or Bugcrowd can facilitate CVD through bug bounty programs, encouraging ethical hackers to report issues.

Detailed Guidance:

- **Establish CVD Policy**: Create a policy with a dedicated email (e.g., security@company.com) or portal, following **ISO 29147** guidelines.
- **Promote Reporting**: Publicise the policy on the company website and developer forums.
- **Respond Promptly**: Acknowledge reports within 7 days and provide updates within 30 days.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Document Policy**: Include the CVD policy, response metrics, and reported vulnerabilities in the technical file.
- **Reward Reporters**: Consider bug bounties to incentivise reporting, using platforms like HackerOne.

Case Study: An SME sets up a CVD portal on HackerOne, receiving and resolving a reported vulnerability within 25 days. The self-assessment documents the policy and response metrics.

Table 13:
Template CVD Policy

Channel	Response Time	Reported Vulnerabilities	Evidence	Status
security@company.com	7 days	3 CVEs	HackerOne report	Resolved

1.2.6. Free Security Updates

Updates must be provided free of charge for a defined support period (e.g., minimum 5 years for IoT devices or for the product's lifetime). SMEs should ensure updates are easy to install, preferably automatically, using OTA mechanisms.

Detailed Guidance:

- **Define Support Period (CRA Art. 13(8)):** Set a support period that reflects the product's expected time in use; it may not be shorter than 5 years, unless the product is reasonably expected to be used for less than 5 years, in which case the support period equals that shorter lifetime. If the product is expected to be used longer than 5 years, set a longer support period**.**
- **Automate Updates**: Use OTA platforms like Mender.io or Balena for seamless updates.
- **Test Updates**: Verify update installation and functionality in a test environment.
- **Document Support**: Include support policies, update logs, and user instructions in the technical file.

- **Monitor Compliance**: Track update deployment and user adoption rates, ensuring no costs are imposed.

According to the CRA requirements, the manufacturer must ensure that each security update remains available to users for a period of at least 10 years from its issuance or for the remaining duration of the support period, whichever is longer. In practice, SMEs should maintain an archive repository of security patches (e.g. on the website or update server) accessible to customers even after the end of official support. Also, if the product evolves through major software versions, the manufacturer must offer users the new versions free of charge and without imposing additional hardware or software costs to benefit from the security fixes (in accordance with art. 13(10) CRA). All these aspects will be documented in the technical file, including the justification for the support period (minimum 5 years) and the way in which users are informed about the end of support or the availability of long-term security updates.

Case Study: A smart thermostat SME commits to 5 years of free updates via Mender.io, documenting the policy and OTA mechanism in the self-assessment.

Table 14:
Template Support Policy

Product	Support Period	Update Mechanism	Last Update	Evidence	Status
Thermostat	5 years	OTA (Mender.io)	2025-07-01	Update log	Compliant

1.3. Recommended Self-Assessment Checklist

To comply with the CRA's obligations on technical documentation and conformity assessment, maintaining a structured self-assessment checklist can provide strong support. We recommend a single checklist that covers all 21 Annex I requirements to track status, evidence, and sign-off over the product lifecycle. The columns for such self-assessment can be:

- **Annex I Ref / Requirement ID (e.g., 1.1.9 Secure Boot)**
- **Product / Version (incl. firmware/software build)**
- **Claim of Conformity (Yes / Partial / No)**
- **Objective Evidence (link/path) (test report, policy, config, SBOM, advisory)**
- **Test/Review Date**
- **Responsible Role / Owner**
- **Deviations & Compensating Controls (if any)**
- **Residual Risk & Rationale**
- **Next Action / Due Date**
- **Approval / Sign-off (name, date)**
- **Tech Doc Reference (where this lives in the Technical Documentation index)**

SMEs can use a compliance dashboard in tools like **Confluence**, **Notion**, or **Excel** to visualise progress, link to evidence, and track remediation.

This checklist is an internal control artifact intended to support CRA compliance (technical documentation, conformity assessment, and post-market monitoring). It does not, by itself, replace any CRA obligation; rather, it organises the evidence you must already produce and maintain.

1.4. Case Study

An SME developing a smart doorbell conducts a self-assessment:

- **Product Requirements**: Uses OWASP ZAP to verify no vulnerabilities, implements TLS 1.3, and disables unused ports. Penetration tests confirm compliance.
- **Vulnerability Handling**: Generates an SBOM with CycloneDX, conducts quarterly OpenVAS scans, and publishes a CVD policy on HackerOne.
- **Outcome**: Achieves full compliance with 18 requirements, identifies gaps in automatic updates, and plans remediation within 3 months, documented in a dashboard.

1.5. Tools and Resources

The examples and capabilities listed in this document are tool-agnostic. They describe what a tool must do, not which brand to use. Teams may use any equivalent solution that provides the stated capability and evidence.

- **Vulnerability Scanning**: OpenVAS, Nessus, Trivy.
- **Penetration Testing**: Metasploit, Burp Suite.
- **Code Analysis**: SonarQube, OWASP Dependency-Check.
- **Logging**: Syslog, ELK Stack, Graylog.
- **SBOM Generation**: Snyk, CycloneDX, SPDX.
- **Standards**: ETSI EN 303 645, NIST SP 800-53, ISO 27001.

This section provides SMEs with a robust, detailed methodology to achieve and document compliance with all essential requirements, supported by practical tools, templates, and case studies.

2. Certification of Products Containing Digital Elements

The **Certification of Products Containing Digital Elements** criterion leverages European cybersecurity certification schemes to demonstrate CRA compliance, aligning with the **Cybersecurity Act (EU) 2019/881**. EU cybersecurity certification schemes exist under the Cybersecurity Act (e.g., EUCC for ICT products), but their role for CRA presumption will be specified by Commission delegated acts under Art. 27(9).

Presumption of conformity (CRA Art. 27(8)–(9)): where the Commission specifies applicable European cybersecurity certification schemes by delegated act under the CRA, products holding an EU statement of conformity or certificate under such a scheme are presumed to conform only to the Annex I requirements covered by that certificate. This section provides an exhaustive methodology for SMEs to assess certification applicability, map CRA requirements to standards, and integrate certifications into the self-assessment, with detailed guidance, case studies, and templates.

2.1. Certification Schemes and Standards

The CRA encourages certifications **like Common Criteria (ISO/IEC 15408)**, **EUCS (EU Cloud Security), ETSI EN 303 645** (for IoT), and **IEC 62443** (for industrial systems). SMEs should evaluate whether their product category is covered by an existing scheme, using resources like **ENISA's certification candidate lists.**

Key Standards:

- **ETSI EN 303 645**: Covers IoT security, including secure configurations, data protection, and vulnerability disclosure.
- **Common Criteria**: Provides assurance levels (EAL1-EAL7) for IT products, suitable for critical systems like firewalls.
- **ISO 27001**: Focuses on organisational security processes, relevant for vulnerability handling.
- **IEC 62443**: Addresses industrial IoT, covering secure development and operation.
- **NIST SP 800-53**: Provides technical security controls, mapping to CRA requirements.

2.2. Self-Assessment Methodology

The self-assessment should include a detailed checklist:

1. **Existing Certifications**: Does the product hold a cybersecurity certification? For example, a smart home device certified under ETSI EN 303 645 covers many CRA requirements.
2. **Applicability**: Is the product eligible for a European certification scheme? Consult ENISA's lists or notified bodies.
3. **Standards Alignment**: Map CRA requirements to standards, identifying overlaps. For example, ISO 27001's A.12.6.1 covers vulnerability handling.
4. **Certification Planning**: Assess the feasibility of pursuing certification, considering costs, timelines, and benefits.
5. **Partial Compliance**: Document adherence to standards, even without full certification, to demonstrate due diligence.

Table 15:
Mapping Example

CRA Requirement	Standard	Clause	Evidence
Secure default configurations	ETSI EN 303 645	Clause 5.1	Configuration report
Vulnerability disclosure	ISO 27001	A.12.6.1	CVD policy

2.3. Practical Steps for SMEs

1. **Identify Relevant Standards**: Use ENISA's website or consult with notified bodies to find applicable standards. For example, a smart meter SME should review IEC 62443.
2. **Document Compliance**: Maintain records of standards adherence, such as ISO 27001 audit reports or ETSI EN 303 645 test results.
3. **Engage Certification Bodies**: Contact accredited bodies listed by ENISA for certification processes.
4. **Leverage Partial Compliance**: Document partial compliance with standards to reduce CRA assessment scope.
5. **Develop Certification Roadmap**: Plan timelines, budgets, and resources for certification. For example, Common Criteria certification may take 6-12 months and cost €50,000-€100,000.

2.4. Case Study

An SME developing a cloud-based IoT platform pursues EUCS certification:

- **Assessment**: Maps CRA requirements to EUCS, identifying overlaps in data protection, encryption, and vulnerability handling.
- **Action**: Engages a notified body (NB), submits test reports (e.g., penetration tests, SBOM), and documents compliance with EUCS clauses.

- **Outcome**: Achieves certification within 9 months, streamlining CRA compliance and enhancing market trust. The self-assessment includes a mapping table and certification report.

2.5. Certification Roadmap Template

Table 16:
Template Certification Roadmap

Certification	Timeline	Cost Estimate	Responsible Party	Evidence	Status
EUCS	9 months (2025-03-01 to 2025-12-01)	€75,000	Security Team	Test reports	In progress

2.6. Tools and Resources

- **ENISA**: Certification candidate lists and notified body directories.
- **Standards**: ETSI EN 303 645, ISO 27001, IEC 62443, Common Criteria.
- **Tools**: Confluence for documentation, Snyk for SBOM generation, OWASP ZAP for testing.

This section ensures SMEs can leverage certifications to simplify CRA compliance, with detailed guidance, templates, and case studies.

3. Product Classification: Compliance Pathways

The **Product Classification** criterion determines the appropriate compliance pathway based on the CRA's risk-based classification of products into Default, Important — Class I (Annex III), Important — Class II (Annex III), and Critical (Annex IV). This section provides an exhaustive methodology for SMEs to classify products, understand compliance obligations, and integrate classification into the self-assessment, with detailed guidance, risk assessment methodologies, and case studies.

Funded by the European Union ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3.1. Understanding Product Classification

The CRA classifies products based on their potential cybersecurity risk, as defined in Annex III and Annex IV:

- **Default — Not listed in Annex III/IV.**
- **Important — Class I (Annex III) —** e.g., operating systems, browsers, VPN, SIEM, routers/modems.
- **Important — Class II (Annex III) —** e.g., hypervisors, container runtimes, firewalls, IDS/IPS.
- **Critical (Annex IV) —** e.g., hardware devices with security boxes, smart-meter gateways, smartcards/secure elements.

Classification is based on the product's use case, data sensitivity, and potential impact on critical infrastructure or user safety.

3.2. Self-Assessment Methodology

The self-assessment should include a detailed decision tree:

1. **Check CRA Annexes**: Review Annex III and IV for product categories. For example, smart home cameras are Class I, while VPN software is Class II.
2. **Assess Risk Impact**: Conduct a risk assessment using **ISO 27005**, **NIST SP 800-30**, or **OCTAVE Allegro** to evaluate the impact of a cyberattack.
3. **Document Classification**: Record the classification, risk assessment results, and justification in the technical file.
4. **Verify Compliance Pathway**: Ensure the correct assessment module (internal control, EU-type examination) is followed based on classification.

Table 17:
Decision Tree Example

Question	Response	Action
Is the product in Annex III or IV?	Yes (Class II)	Engage notified body for EU-type examination
Could failure impact critical infrastructure?	No	Classify as default or Class I, use internal control

3.3. Compliance Pathways

- **Default products** — Module A (Internal control of production). Manufacturer self-assesses conformity with all 21 Annex I requirements and keeps full technical documentation.
- **Important — Class I —** Module A only if harmonised standards/common specifications or an applicable EU cybersecurity certification scheme (assurance ≥ "substantial") are applied; otherwise third-party assessment (Modules B + C or H) is required for the uncovered requirements.
- **Important — Class II** — Third-party assessment mandatory (Modules B + C or H) or an applicable EU cybersecurity certification scheme (assurance ≥ "substantial"); Module A is not permitted.
- **Critical (Annex IV)** — Where designated by delegated act, EU cybersecurity certification is mandatory (assurance level as specified). Until such designation, apply Art. 32(3) (same options as Important — Class II).

3.4. Practical Steps for SMEs

1. **Classification Checklist**: Develop a checklist to verify if the product matches Class I or II criteria, including questions on data sensitivity, infrastructure impact, and Annex listings.
2. **Risk Assessment**: Use OCTAVE Allegro or NIST SP 800-30 to assess risks, focusing on likelihood and impact. For example, assess risks like data breaches or device tampering.
3. **Compliance Planning**: For Class II, identify notified bodies (e.g., via ENISA) and budget for audits (€50,000-€150,000). For default/Class I, schedule internal audits.

4. **Documentation**: Include classification reports, risk assessments, and compliance plans in the technical file.
5. **Regular Reviews**: Reassess classification annually to account for product updates or new CRA guidance.

Table 18:
Template Risk Assessment

Threat	Likelihood	Impact	Risk Level	Mitigation	Evidence
Unauthorised access	Medium	High	High	MFA	Test report 2025-07-01

3.5. Case Study

An SME developing a password manager (Class I) classifies it based on Annex III, conducts a NIST SP 800-30 risk assessment (identifying risks like credential theft), and engages a notified body for EU-type examination. The self-assessment documents the classification, risk assessment, and audit preparation, ensuring compliance with CRA requirements.

3.6. Tools and Resources

- **Risk Assessment**: OCTAVE Allegro, NIST SP 800-30, ISO 27005.
- **Documentation**: Confluence, SharePoint.
- **Notified Bodies**: ENISA directory.

This section suggests a practical, tool-agnostic workflow that SMEs can use to classify products and choose an appropriate CRA conformity-assessment pathway. It is one option to support compliance; organisations may use an equivalent workflow if it yields the same decisions and evidence. The steps and artifacts above are recommendations, not CRA-mandated methods. Where this document mentions a "risk assessment tool," read it as a placeholder for any method that produces the capability outcomes listed (e.g., a qualitative risk matrix or a lightweight scoring sheet).

This guidance will be updated as EU implementing/delegated acts and certification schemes are finalised. Until then, treat the workflows above as **illustrative options** to structure internal classification and evidence collection.

4. Technical Documentation and Risk Assessment

The **Technical Documentation and Risk Assessment** criterion ensures SMEs produce comprehensive documentation to demonstrate CRA compliance. The CRA requires a technical file for each product, including product descriptions, risk assessments, security measures, test reports, and user guidance. This section provides an exhaustive methodology for compiling and assessing documentation, with detailed guidance, templates, and case studies.

4.1. Documentation Requirements

The technical file must include:

1. **Product Description**: Detailed specifications, functionality, and intended use.
2. **Risk Assessment**: Comprehensive analysis of threats and mitigations, aligned with **ISO 27005** or **NIST SP 800-30**.
3. **Essential Requirements Compliance**: Evidence of compliance with all 21 requirements, including test reports and policies.
4. **Test Reports**: Results of vulnerability scans, penetration tests, and code reviews.
5. **Secure Development Lifecycle (SDLC)**: Policies for secure coding, testing, and review, aligned with **OWASP SAMM** or **Microsoft SDL**.
6. **User Guidance**: Manuals or online help sections explaining cybersecurity features, such as update installation and vulnerability reporting.

4.2. Self-Assessment Methodology

1. **Documentation Checklist**: Verify the presence of all required documents, including product descriptions, risk assessments, and test reports.
2. **Risk Assessment Process**: Use **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) or **PASTA** (Process for Attack Simulation and Threat Analysis) to identify threats.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3. **Evidence Collection**: Gather test reports (e.g., Nessus, Metasploit), SBOMs, and SDLC policies.
4. **Organise Technical File**: Use document management systems like **Confluence**, **SharePoint**, or **Notion** for accessibility and audit-readiness.
5. **Regular Updates**: Schedule quarterly reviews to update documentation, reflecting product changes or new vulnerabilities.

Table 19:
Template Documentation Checklist

Document	Required	Status	Evidence	Gaps	Action
Product Description	Yes	Complete	Specification V1.2	None	N/A
Risk Assessment	Yes	Partial	STRIDE report	Missing mitigation details	Complete by 2025-08-01

4.3. Practical Steps for SMEs

1. **Develop Product Description**: Detail hardware, software, connectivity, and use case. For example, a smart thermostat description includes Wi-Fi protocols and data processing.
2. **Conduct Risk Assessment**: Use STRIDE to identify threats like unauthorised access or data tampering. Document mitigations like encryption or access controls.
3. **Collect Evidence**: Compile test reports from tools like Nessus, OWASP ZAP, or SonarQube. Include SBOMs and SDLC policies.
4. **Organise Documentation**: Use Confluence to create a structured technical file, with folders for descriptions, assessments, and reports.
5. **Provide User Guidance**: Develop manuals with clear cybersecurity instructions, using templates from **ETSI EN 303 645**.

4.4. Case Study

An SME producing a smart camera compiles a technical file:

- **Product Description**: Details camera specs, Wi-Fi connectivity, and cloud storage.
- **Risk Assessment**: Uses STRIDE to identify threats like unauthorised streaming, mitigated with TLS 1.3 and MFA.
- **Test Reports**: Includes Nessus scan results and penetration test reports.
- **SDLC**: Adopts OWASP SAMM, documenting secure coding practices.
- **User Guidance**: Provides a manual with update instructions and a CVD email.
- **Outcome**: The self-assessment verifies completeness, identifies gaps in SDLC documentation, and plans remediation within 6 months.

4.5. Tools and Resources

- **Risk Assessment**: STRIDE, PASTA, NIST SP 800-30.
- **Testing**: Nessus, OWASP ZAP, Metasploit.
- **Documentation**: Confluence, SharePoint, Notion.
- **Standards**: OWASP SAMM, Microsoft SDL, ETSI EN 303 645.

This section ensures SMEs have a complete, audit-ready technical file, with detailed methodologies and templates.

5. Conformity Assessment Process and EU Declaration of Conformity

The **Conformity Assessment Process and EU Declaration of Conformity** criterion finalises CRA compliance, ensuring SMEs follow the appropriate assessment module and issue a valid Declaration of Conformity. This section provides an exhaustive methodology for navigating this process, addressing post-market obligations, and preparing the Declaration, with detailed guidance, templates, and case studies.

5.1. Conformity Assessment Modules

The CRA applies the following Annex VIII modules:

- **Module A** — Internal control of production. Manufacturer self-assesses compliance with all 21 requirements; maintains technical documentation and a declaration of conformity. (Used for Default; for Class I only under the conditions in point 3.3.)
- **Module B** — EU-type examination. A notified body evaluates a representative product "type" against applicable requirements.
- **Module C** — Conformity to type based on internal production control. Manufacturer ensures production conforms to the "type" approved in Module B.
- **Module H** — Full quality assurance. A notified body assesses and monitors the manufacturer's full quality system (design and production) for the applicable requirements.

As summarised in point 3.3, when applied to the different product classes, this means:

- **Default**: Module A.
- **Important — Class I**: Module A only if harmonised standards/common specifications or an applicable EU certification scheme (≥ "substantial") are applied; otherwise B + C or H.
- **Important — Class II**: B + C or H, or an applicable EU certification scheme (≥ "substantial"); Module A not permitted.
- **Critical (Annex IV):** EU certification mandatory when designated by delegated act; until then, follow Art. 32(3) (same as Important — Class II).

5.2. Self-Assessment Methodology

1. **Determine Module**: Identify the required module based on classification (default, Class I, or Class II).
2. **Conduct Internal Assessments**: For default and Class I, verify compliance with all requirements using the self-assessment checklist.
3. **Engage Notified Bodies**: For Class II, submit the technical file to a notified body and address audit findings.
4. **Address Post-Market Obligations**: Monitor vulnerabilities, issue updates, and maintain documentation throughout the product's lifecycle.
5. **Issue Declaration**: Sign the EU Declaration of Conformity, affirming compliance with CRA requirements.

Table 20:
Template EU DoC

EU Declaration of Conformity
Product: [Product Name] Manufacturer: [Company Name, Address] We hereby declare that the above product complies with Regulation (EU) 2024/2847 (Cyber Resilience Act). Essential Requirements: Fully compliant with Annex I. Conformity Assessment: [Module, e.g., Internal Control of Production] Standards Applied: [e.g., ETSI EN 303 645, ISO 27001] Date: [YYYY-MM-DD] Signed: [Name, Title]

5.3. Practical Steps for SMEs

1. **Verify Classification**: Confirm the product's class to determine the assessment module.
2. **Conduct Internal Audits**: Use the self-assessment checklist to verify compliance, supported by test reports and documentation.
3. **Engage Notified Bodies**: For Class II, contact accredited bodies (e.g., via ENISA), submit the technical file, and prepare for audits.
4. **Monitor Post-Market**: Use tools like Snyk or NIST's NVD to track vulnerabilities, issuing patches as needed.
5. **Issue Declaration**: Draft and sign the Declaration of Conformity, including it in the technical file.

5.4. Case Study

An SME developing a Class I smart toy conducts an internal audit, verifying compliance with all 21 requirements using Nessus and OWASP ZAP reports. The self-assessment confirms documentation completeness, leading to a signed Declaration of Conformity. For a Class II firewall, the SME engages a notified body, submits test reports, and addresses audit findings within 3 months, documenting the process.

5.5. Tools and Resources

- **Auditing**: Confluence for audit tracking, Nessus for testing.
- **Notified Bodies**: ENISA directory.
- **Standards**: ETSI EN 303 645, ISO 27001.

This section ensures SMEs complete the conformity assessment process and maintain compliance, with detailed methodologies and templates.

Conclusion

This methodological compliance assessment framework provides **support to SMEs' implementation of the EU Cyber Resilience Act**, through in-depth guidance, practical examples, case studies, and tools on **five key criteria** of the CRA: (1) Essential Cybersecurity Requirements Compliance, (2) Certification of Products with Digital Elements, (3) Classification of Products as Class I or Class II and Corresponding Actions, (4) Technical Documentation Completeness, and (5) Overall Conformity Assessment Procedures. Aligned with the objectives of the **SECURE Project**, the guidance aims to make CRA obligations tangible through recommendations based on recognised approaches and best practices in the cyber domain; however, remaining suggestive. Based on the future developments in the CRA's legal context, the guideline may be subject to change. As next steps for SMEs, it is recommended to consult additional guidelines on the **SECURE repository**, such as **The CRA's Essential Cybersecurity Requirements: Annex I, Part I** for practical suggestions and recommendations for each of the Annex I stipulations, as well as **CRA 101: Understanding CRA Obligations** for a condensed overview of your legal obligations under the CRA.