## Guide on vulnerability handling and cyber resilience principles: supporting CRA compliance for SMEs

### Background and motivation

The Cyber Resilience Act (CRA) introduces new legal obligations for cybersecurity-by-design across products with digital elements, directly impacting many SMEs. However, SMEs often lack in-house capacity to track standardisation developments or understand how to use standards to demonstrate compliance. This guide addresses this by empowering SMEs with clear, structured and practical information that links standardisation with EU regulation, with the goal of making standards accessible, usable, and inclusive for SMEs.

As emphasized in the EU Cybersecurity Strategy, standards should play a critical role in boosting the EU's cybersecurity resilience and regulatory capacity. To ensure smooth adoption of harmonised standards by European SMEs, this guide presents them in a clear, simplified, and structured way, helping non-experts navigate them effectively. Increased readiness of companies in implementing CRA standards will improve overall cybersecurity resilience and readiness in the EU.

This guide focuses on horizontal standards, specifically prEN 40000-1-2 (Cyber Resilience Principles) and prEN 40000-1-3 (Vulnerability Handling) because they offer broad applicability across industries, scalability for limited resources, and clear, actionable processes that SMEs can adopt without heavy investment. At the time of writing the two standards are also further advanced in the standardisation process by being in the enquiry stage, making them less likely to encounter bigger changes before their publication. This means that the guide can offer a valuable head start to SMEs in engaging with standards supporting the CRA early on, gaining a competitive advantage in initiating their compliance journey sooner.

### Outline: CRA standards guide for SMEs

1. Introduction

- Purpose: Guide SMEs in implementing prEN 40000-1-2 (cyber resilience) and prEN 40000-1-3 (vulnerability handling) to comply with the Cyber Resilience Act (CRA).
- Scope: Focus on processes, teaching how to apply the standards in practice without relying on specific tools or solutions.
- Audience: SMEs with limited resources that place a "product with digital elements" on the market and will be subject to CRA requirements.

2. Regulatory and Standardisation Context

2.1 Key Concepts & Regulatory Context

- Definitions:
    - Risk, vulnerability, SBOM (Software Bill of Materials), security by design, secure by default, coordinated vulnerability disclosure (CVD).
- CRA Overview:
    - Essential requirements (Annex I, Parts I & II).
    - How the standards align with CRA obligations.

2.2 Overview of the CRA's Standardisation Context

- An introduction to the role of standards in CRA compliance.
- Horizontal vs. vertical standards and their relevance to SMEs.
- The concept of presumption of conformity and its importance for manufacturers.

2.3 Relevant Published, Draft, or Upcoming Harmonised Standards

- A categorised list of key standards (horizontal, vertical, and supporting).
- Brief descriptions of their focus areas and relevance to SMEs.
- Guidance on how SMEs can identify and select the most applicable standards for their products.

3. Cyber Resilience for SMEs (prEN 40000-1-2)

3.1 Risk-Based Approach

- Process:
    - Identify and document the product context (intended use, operational environment, user profiles).
    - Conduct a risk assessment: Identify assets, threats, and vulnerabilities.
    - Apply a risk treatment plan (avoidance, mitigation, acceptance, transfer).
- SME Adaptation:
    - Simplify risk assessment using qualitative methods (e.g., risk matrices).

    - Focus on high-impact assets (e.g., user data, critical functions).
- Short example: Risk assessment for a small IoT device.

3.2 Security by Design & Default

- Process:
    - Integrate cybersecurity from conception to decommissioning.
    - Apply principles: least privilege, attack surface minimization, defense in depth.
    - Ensure secure default configurations (e.g., auto-updates, disabled unnecessary features).
- SME Adaptation:
    - Document security decisions in the product design phase.
    - Align with state of the art and regulatory requirements.
- Short example: Secure design process for a cloud-connected product.

3.3 Transparency & Communication

- Process:
    - Communicate risks and mitigation measures clearly and accessibly.
    - Provide user-friendly advisories and instructions.
- SME Adaptation:
    - Use plain language and multilingual summaries.
    - Ensure accessibility for all users (e.g., simple formats, clear visuals).
- Short example: Drafting a user advisory for a security update.

3.4 Practical Implementation

- Document the product context (intended purpose, foreseeable use, operational environment).
- Perform threat modeling to identify potential risks.
- Select cybersecurity controls based on risk level and product requirements.

4. Vulnerability Handling for SMEs (prEN 40000-1-3)

4.1 Preparation

- Process:
    - Develop a vulnerability handling policy (internal) and coordinated vulnerability disclosure (CVD) policy (external).
    - Create and maintain an SBOM (Software Bill of Materials) for all software components.
    - Establish secure communication channels for receiving and disclosing vulnerabilities.
- SME Adaptation:
    - Start with a basic SBOM covering top-level dependencies.
    - Define roles (e.g., point of contact for vulnerability reports).
- Short example: Creating an SBOM for a firmware-based product.

4.2 Receipt & Verification

- Process:
    - Monitor internal and external sources for vulnerability reports (e.g., databases, user reports).
    - Verify reports: Assess credibility, reproducibility, and applicability.
    - Prioritize vulnerabilities based on risk and impact.
- SME Adaptation:
    - Use a structured process to triage and document reports.
    - Assign severity levels (e.g., critical, high, medium).
- Short example: Triaging a vulnerability report for a web application.

4.3 Remediation & Release

- Process:
    - Develop fixes or mitigations (e.g., patches, configuration changes).
    - Test remediations for effectiveness and compatibility.
    - Release updates securely (e.g., signed packages, HTTPS).
    - Publish advisories in human- and machine-readable formats.

- SME Adaptation:
    - Separate security updates from functional updates where feasible.
    - Provide clear installation instructions for users.
- Short example: Releasing a security update for a SaaS platform.

4.4 Post-Release

- Process:
    - Monitor the effectiveness of fixes and gather user feedback.
    - Document lessons learned to improve future vulnerability handling.
- SME Adaptation:
    - Schedule regular reviews of the vulnerability handling process.
    - Update policies and procedures based on feedback.
- Short example: Post-release review for a patched embedded system.

5. Practical Examples (possible suggested topics but subject to change)

- Case Study 1: Risk management for a small medical device manufacturer.
- Case Study 2: Vulnerability handling process for a software developer.
- Case Study 3: SBOM creation and CVD for a smart home product.

6. Conclusion & Next Steps

- Key Takeaways:
    - Where to start from (e.g. with risk assessment and SBOM creation)
    - Focus on processes, not specific tools to adapt standards to your SME's context.
    - Prioritize transparency and secure communication.
- Call to Action:
    - Assign a cybersecurity champion in your organization.
    - Pilot a risk assessment for one product.

    - Engage with standardisation activities and standards development: resources by SBS, DIGITAL SME

Appendices:

- Glossary of terms.
- Checklists for risk assessment and vulnerability handling.
- Mapping to CRA Requirements
- Further reading.

Annex III example: Mapping to CRA Requirements

| CRA Annex I Requirement | prEN 40000-1-2 | prEN 40000-1-3 |
|---|---|---|
| Risk-based cybersecurity | Clause 6 | 5.5.3 |
| Secure by default | 5.4 | 5.7.2 |
| Vulnerability handling | 7.8 | Clause 5 |
| SBOM | – | 5.3.8 |
| Transparency | 5.5, 6.6 | 5.7.3 |