STAN4CR

Cybersecurity requirements for products with digital elements — Principles for cyber resilience

This standard is intended to cover the first Essential Requirement of the CRA Annex I part I (1), ensuring that Products with Digital Elements (PwDE) are designed, developed and produced with an appropriate level of cybersecurity in mind.

To meet the standardization request, the standard has to address several factors:

01 The standard needs to be horizontal, meaning that it should be applicable to all products with digital elements under the CRA and cover their entire lifecycle.

02 Most of the manufacturers can apply this standard when doing self-assessment for the activities in their organization, which will support them implementing the essential requirements of the CRA.

03 The standard proposes to meet the Essential Requirement of the CRA Annex I part I (1) by addressing four main principles:

- 'Risk-based approach' to address the risk-based part of the request.
- 'Secure by design' to ensure the design, development, production, and disposal are secure over the products lifecycle.
- 'Secure by default' to ensure that a user's lack of knowledge does not compromise the security of the PwDE;
- 'Transparency' to ensure users and supply chain partners are aware of risks.

04 The standard should serve as a framework, providing elements for the vertical standards to facilitate coherence between the vertical standards. The horizontal standards are meant to be broadly applicable across the full scope of the CRA.

05 The standard will provide elements of good risk management to ensure the risk-based approach is applied in a coherent manner

06 To ensure that security is maintained during the full life cycle, the standard will provide a number of activities the output of which should prove that the product is capable of compliance with the Essential Requirement of the CRA Annex I part I (1). This standard is therefore a 'process standard'. Process standards are known for helping organizations, industries, and professionals maintain uniformity in their operations and achieve desired outcomes.

CEN CENELEC European Commission EFTA

For more information

www.cencenelec.eu

STAN4CR

Cybersecurity requirements for products with digital elements – Vulnerability Handling

To fulfil the Cyber Resilience Act (CRA) Standardization Request, the standard shall provide clear specifications for **vulnerability handling activities,** covering all relevant product categories.

These activities are to be implemented by manufacturers of products with digital elements and will enable manufacturers to comply with the vulnerability handling requirements outlined in the CRA.

The standard under development will align with the internationally recognized state of the art for vulnerability management, specifically ISO/IEC 29147:2018 and EN ISO/IEC 30111:2019, and it will include the following activities:

- Sharing
- Preparation
- Discovery
- Validation and Triage
- Remediation
- Raising Awareness
- Promoting Deployment
- Post-release

CEN CENELEC

European Commission

EFTA

For more information

www.cencenelec.eu