Nemko Digital

Mastering CRA - Cyber Resilience Act Practical Steps for Trustworthy Systems - Webinar Report

---

Executive Summary

Nemko Digital hosted the "Mastering the Cyber Resilience Act" webinar, attracting over 300 industry professionals eager to understand the implications of this landmark EU regulation. The session, moderated by Bas Overtoom, featured expert insights from Pepijn van der Laan and Daniel Breive Havre. The primary objective was to demystify the Cyber Resilience Act (CRA), providing a clear roadmap for manufacturers to achieve compliance for their products with digital elements. The discussion covered the CRA's timeline, scope, and essential requirements, practical steps for testing and validation, and strategic approaches for embedding cybersecurity practices within organizations.

The Cyber Resilience Act: A Deep Dive

Dr. Pepijn van der Laan initiated the core discussion by positioning the CRA within the broader framework of EU digital regulations, which includes the AI Act, Data Act, and NIS2 Directive. He emphasized that the CRA is a critical piece of this puzzle, designed to reduce cybersecurity vulnerabilities across the lifecycle of products with digital elements—encompassing both hardware and software.

Nemko Digital

Main Theme and Objectives

The central theme of the webinar was proactive compliance. The CRA mandates a fundamental shift from reactive security fixes to a "secure-by-design" and "secure-by-default" philosophy. Its objectives are twofold: to ensure products placed on the EU market are secure out-of-the-box and to hold manufacturers responsible for the cybersecurity of their products for a support period of at least five years post-sale. This includes managing vulnerabilities throughout the supply chain, making the Software Bill of Materials (SBOM) a cornerstone of compliance.

Key Timelines and Product Categories

Two critical deadlines were highlighted for manufacturers:

Deadline	Requirement
September 11, 2026	Mandatory reporting of actively exploited vulnerabilities and severe security incidents to ENISA.
December 11, 2027	Full CRA compliance becomes mandatory. Non-compliant products can no longer be sold in the EU.

Dr. van der Laan explained the CRA's risk-based classification of products, which determines the path to conformity:

- **Default Products:** The vast majority of products fall into this category and can undergo a self-declaration of conformity.
- **Important Products (Class I & II):** These include items like operating systems, password managers, and smart home devices. They require a third-party conformity assessment by a notified body.
- **Critical Products:** A smaller, high-risk group including hardware security modules and smart meter gateways, which may require a cybersecurity certificate.

Preparing for Testing and Validation

Daniel Breive Havre provided a practical overview of the testing and certification process. He stressed that while many harmonized standards are still in

development, the essential requirements are already outlined in Annex I of the CRA, allowing companies to begin their compliance journey immediately.

Essential Requirements (Annex I)

The requirements are split into two main parts:

1. **Product Requirements:** These focus on the technical security of the product itself, mandating features like secure-by-default configurations, protection against unauthorized access, data minimization, integrity and confidentiality of data, and mechanisms for secure updates.
2. **Vulnerability Handling Requirements:** These are process-oriented, requiring manufacturers to have systems in place to identify and document vulnerabilities (including maintaining an SBOM), provide security updates without delay, and establish clear channels for coordinated vulnerability disclosure.

The Evaluation Process

Mr. Havre outlined a typical two-step evaluation process:

1. **Documentation Review:** Evaluators first assess the manufacturer's documentation, which includes the risk assessment, security development lifecycle processes, vulnerability handling procedures, and the SBOM. He warned attendees not to underestimate the comprehensive nature of this documentation requirement.
2. **Functional Testing & Verification:** This involves hands-on testing to verify the security claims. Examples included using tools like Wireshark to confirm the use of secure communication protocols (e.g., TLS 1.2) and Nmap to scan for open ports and undocumented services, thereby identifying potential attack surfaces.

Strategic Approach to CRA Compliance

The speakers presented Nemko's phased approach to help organizations, from large multinationals to smaller enterprises, navigate the path to compliance.

1. **Discovery & Alignment:** For larger organizations, a foundational workshop is recommended to create a shared understanding of the CRA's impact across different departments (e.g., Product Management, R&D, Legal, IT).

Nemko Digital

2. **Applicability & Requirements:** This phase involves creating an "applicability matrix" to map specific products to the regulatory scope and identify all relevant requirements.
3. **Gap Analysis & Roadmap:** An assessment of current policies, processes, and technical controls against the CRA requirements to identify gaps and create a prioritized remediation roadmap.
4. **Remediation & Support:** Implementing the necessary changes, which can be supported by external experts to accelerate the process.
5. **Validation, Testing & Certification:** The formal process of verifying and certifying compliance.

An interesting insight from a live poll conducted during the webinar revealed that approximately 70% of attendees are in the early stages of their CRA journey, indicating a significant need for structure and support across the industry.

Key Insights from the Q&A Session

The interactive Q&A session addressed several common concerns from the audience:

- **Relationship with RED:** For products already certified under the Radio Equipment Directive (RED), Mr. Havre clarified that this covers a significant portion (~80%) of the CRA's *product-specific* requirements. However, the CRA introduces substantial new *process* requirements for vulnerability handling and secure development that are not covered by RED.
- **Existing Products:** Any product, regardless of its initial release date, must be CRA-compliant if it continues to be sold on the EU market after December 11, 2027.
- **Gap Assessment without Final Standards:** Dr. van der Laan advised that companies should not wait. Gap assessments can be performed against the official text of the CRA and the available draft standards, allowing for the implementation of "no-regret" security improvements while monitoring the finalization of harmonized standards.
- **Role of ISO 27001:** Having an ISO 27001 certified information security management system is highly beneficial as it provides a strong foundation for the CRA's process requirements. However, the CRA has a more specific focus on product security and lifecycle management, which will require additional controls.

Nemko Digital

Conclusion and Next Steps

The webinar concluded with a clear call to action: the time to start preparing for the Cyber Resilience Act is now. With the first major deadline in September 2026, waiting for finalized standards is not a viable strategy. The speakers emphasized that a proactive, structured approach is essential to manage the complexity of the regulation and ensure continued market access in the European Union.

For attendees, the key takeaway is that CRA compliance is not merely a technical challenge but a strategic imperative that requires cross-functional collaboration, from engineering and product management to legal and compliance teams. Nemko encouraged participants to leverage the available resources, including a follow-up webinar on April 8, 2026, and to begin their internal discovery and gap analysis processes as soon as possible to build a robust and defensible compliance program.

Nemko Digital