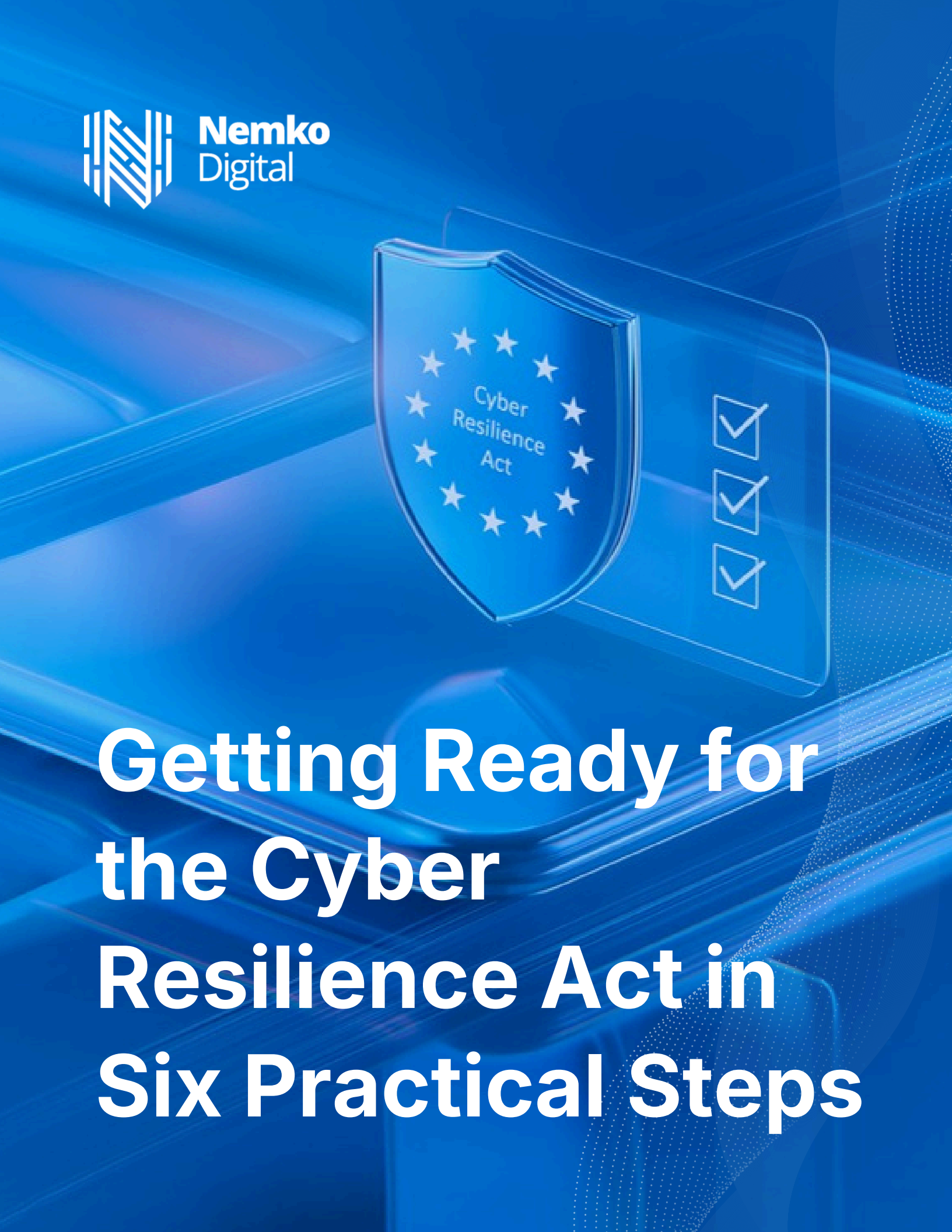
Nemko Digital



Getting Ready for the Cyber Resilience Act in Six Practical Steps

The Cyber Resilience Act (CRA) will significantly change how digital products are developed, maintained, and placed on the European market. The regulation introduces mandatory cybersecurity requirements for products with digital elements, including connected devices, embedded software, and cloud-connected services.

To ensure proportionate security obligations, the CRA classifies products into Class I and Class II categories. Class I covers the majority of products and allows manufacturers to rely on internal controls and self-assessment. Class II includes products with higher cybersecurity relevance and requires more rigorous conformity assessment procedures, often involving a notified body. This classification directly impacts the level of assurance, documentation, and compliance pathway required.

Although the CRA entered into force in December 2024, many organizations underestimate how quickly the key milestones are approaching. Requirements related to vulnerability and incident reporting will apply from September 2026, while the full set of obligations will apply to all products placed on the EU market from December 2027.

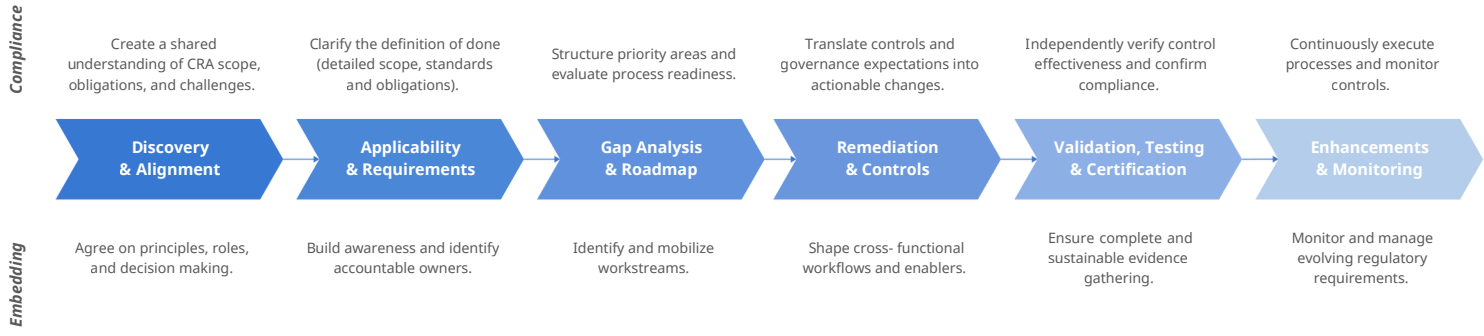
For companies developing complex digital products, this timeline is shorter than it may appear. Achieving compliance requires more than documentation. It demands changes to engineering practices, governance structures, and product lifecycle management.

While CRA is often interpreted at the product level, compliance cannot be achieved product by product in isolation, particularly in organizations managing large portfolios. Companies with hundreds or thousands of products must embed cybersecurity, compliance processes, and governance models at the organizational level to ensure consistency and scalability.

At Nemko Digital, we therefore take a holistic approach. CRA readiness is not only about making individual products compliant, but about establishing shared processes, clear ownership, and enabling tooling that allow compliance to be executed consistently across teams and product lines. The six steps below describe the product compliance journey, but their success depends on how effectively they are embedded into organizational structures and operational practices.

Nemko's CRA Readiness Approach

A phased approach to interpret, remediate, validate, and continuously manage regulatory obligations.



1. Discovery and Alignment

The first step in preparing for the CRA is establishing a shared understanding of how the regulation applies to the organization. This typically requires alignment between product teams, cybersecurity specialists, legal advisors, and executive leadership.

Organizations must determine which products fall within scope and what role they play under the regulation. These roles, such as manufacturer, importer, or distributor, define the specific responsibilities an organization must fulfil.

In larger organizations, this step also establishes the foundation for scaling CRA compliance across multiple product lines, ensuring that governance and ownership models can be consistently applied rather than redefined for each product.

Activities in this stage usually include:

- Identifying products with digital elements that fall within CRA scope
- Clarifying regulatory roles and responsibilities
- Determining whether products fall into Class I or Class II categories
- Establishing governance structures and decision-making processes

For example, a manufacturer of smart home thermostats might begin by mapping all products sold in the EU, including the device firmware, mobile application, and associated cloud services. During this exercise, the company can determine that its devices fall into the Class I category rather than Class II, which influences how compliance and certification will be approached later.

The way to Demonstrate conformity differs by product category

Cybersecurity certificate	Comformity assessment	Vertical standards	Self- declaration

Critical products[1]

- Hardware devices with security boxes
- Smart meter gateways within smart metering systems
- Smartcards

Important products[1]

Class I

- Identity management systems
- Browsers
- Password managers
- Malware protection software
- VPN products
- Network management systems
- SIEM systems
- Boot managers
- Key/certificate issuance software
- Network interfaces
- Operating systems
- Routers, modems and switches
- Microprocessors with security function
- Microcontrollers with security function
- ASIC & FPGA with security function
- Smart home GP VAs
- Smart home products with security functionalities
- Internet connected toys
- Personal wearables for health monitoring

Class II

- Hypervisors and container runtime systems
- Firewalls
- Tamper- resistant microprocessors
- Tamper- resistant microcontrollers

Default products

- All the rest

[1] Implementing regulation (EU) 2025/2392 provides the official technical description of the categories of important and critical products with digital elements, as required by the CRA.

© 2026 All rights reserved by Nemko Digital: content and materials are not to be distributed or shared without prior permission.

2. Applicability and Requirements

Once scope and governance are defined, organizations must translate regulatory obligations into concrete operational requirements. The CRA defines essential cybersecurity requirements that apply across the entire product lifecycle.

These requirements address areas such as secure development practices, vulnerability management, transparency toward users, and the ability to provide security updates throughout the product support period. At this stage, organizations should define what compliance means in practical terms by establishing a clear definition of done for CRA readiness.

Typical activities include:

- Mapping CRA requirements to internal policies and development processes
- Identifying applicable technical standards and security frameworks
- Determining additional obligations for high-risk products
- Assigning accountable owners for each requirement

The distinction between Class I and Class II products becomes important here. Class II products must meet stricter requirements and may require more comprehensive documentation and assurance processes.

For instance, a manufacturer of wearable fitness devices might translate CRA requirements into specific development checkpoints, such as mandatory threat modelling and security testing. If the company were developing a product categorized as Class II, it might also need to align its development processes with additional standards to support future certification.

Standards Are Evolving, Preparation Should Not Wait

At this stage, many organizations raise questions about the availability of harmonized technical standards that will support CRA compliance. These are still under development, with the official deadline for their publication set for 16 July 2027. However, the overall direction of these standards is already clear. They are expected to build on existing best practices in secure development, vulnerability management, and product lifecycle security, which many organizations are already familiar with.

This means organizations should not wait for the final standards to begin their preparation. Leading companies are already aligning their processes with established frameworks and implementing core capabilities such as security by design, vulnerability handling, and documentation practices. Starting now allows organizations to build maturity progressively and avoid compressed timelines as regulatory deadlines approach.

3. Gap Analysis and Roadmap

With requirements clarified, organizations should evaluate their current level of readiness. Many companies already have security practices in place, but these practices may not fully address CRA expectations or may lack the documentation needed to demonstrate compliance.

A structured gap analysis compares existing processes and controls against CRA requirements. This assessment identifies where improvements are necessary and helps prioritize remediation efforts.

Typical focus areas include:

- Integration of cybersecurity requirements into development processes
- Maturity of vulnerability management and disclosure practices
- Availability of technical documentation and compliance evidence
- Readiness for potential third-party conformity assessments

The roadmap that follows will differ depending on whether products fall into Class I or Class II categories. Class II products typically require more extensive preparation for external conformity assessments and certification procedures.

At an organizational level, this phase often reveals fragmentation across teams, for example where different business units follow inconsistent security practices or documentation standards. Addressing these inconsistencies is critical to enabling a scalable compliance approach.

For example, a manufacturer of connected industrial sensors may discover that while security testing is already performed, the organization is not prepared for an external conformity assessment that could apply to certain product categories. The resulting roadmap might therefore include strengthening documentation and preparing processes for third-party audits.



4. Remediation and Controls

Once priorities have been defined, organizations can begin implementing the controls and operational changes needed to meet CRA expectations. This phase focuses on embedding cybersecurity practices into development and operational workflows.

Implementing these changes often requires close collaboration between engineering, security, product management, and compliance teams.

Typical initiatives include:

- Integrating security by design principles into development workflows
- Implementing Software Bill of Materials management capabilities
- Establishing coordinated vulnerability disclosure processes
- Strengthening governance procedures for product security risk management

For example, a company developing connected medical devices may introduce automated security scanning into its software development pipeline. Every time the software is updated, the process can automatically generate a Software Bill of Materials and check for known vulnerabilities in third-party components. These measures help ensure the product meets both regulatory expectations and internal security standards.

For organizations with large product portfolios, standardization is key. Controls should be implemented in a way that they can be reused across teams through shared frameworks, templates, and tooling.



5. Validation, Testing and Certification

Before products can be placed on the EU market, manufacturers must demonstrate that they meet CRA cybersecurity requirements. The level of conformity assessment required depends on whether the product falls into Class I or Class II.

Standard products typically allow manufacturers to perform internal conformity assessments and self-declare compliance. Class II products, however, may require independent evaluation by accredited third-party conformity assessment bodies before they can be placed on the market.

This stage focuses on verifying the effectiveness of implemented controls and preparing the documentation required for regulatory assurance.

Key activities typically include:

- Conducting security testing and product risk assessments
- Reviewing technical documentation and compliance evidence
- Preparing the EU Declaration of Conformity
- Supporting CE marking where applicable

For example, a manufacturer of network routers preparing a new device for the European market may conduct penetration testing on the router firmware and connectivity interfaces. If the device falls into a Class II category, the results of these tests and the associated documentation may be reviewed by an external certification body as part of the conformity assessment process.



6. Enhancements and Monitoring

CRA compliance does not end when a product is released. Manufacturers must maintain cybersecurity throughout the product lifecycle and respond to vulnerabilities that may arise after deployment.
Organizations must therefore establish operational processes that support continuous monitoring and response.

Key capabilities include:

- Monitoring vulnerabilities affecting deployed products
- Issuing security updates during the defined support period
- Reporting actively exploited vulnerabilities and significant incidents
- Tracking evolving regulatory requirements

At scale, this requires centralized oversight combined with distributed execution. Organizations must ensure that monitoring, reporting, and response processes are consistently applied across all products, while still allowing individual teams to operate efficiently.

For example, a company producing connected electric vehicle charging stations may need to monitor vulnerabilities in the software components used in its systems. If a critical vulnerability is discovered, the company must assess the impact, develop a patch, distribute the update, and where required report the incident under CRA reporting obligations.



From Compliance to Digital Trust

The Cyber Resilience Act represents a significant shift in how cybersecurity is regulated within the European digital market. Cybersecurity is becoming a prerequisite for market access for many digital products.

Organizations that begin preparing early can integrate security practices into their engineering processes and product lifecycle management. This not only reduces regulatory risk but also strengthens product resilience and customer trust. Companies that delay preparation may face compressed timelines, costly engineering changes, and potential disruptions to product launches.

In practice, the right starting point depends on the organization's current level of maturity and alignment.

- For many larger organizations, the first priority is to establish internal alignment before moving into detailed implementation. This typically involves clarifying which products are in scope, defining responsibilities across teams, and setting up governance structures that enable compliance to scale across the organization.
- Where this foundation is already in place, organizations can move more directly into translating CRA requirements into internal standards and assessing current capabilities against those expectations. This allows them to identify gaps, prioritize actions, and begin structured remediation.
- From there, organizations can progress through the remaining steps, focusing on implementation, validation, and the establishment of sustainable monitoring capabilities.

Taking a structured and phased approach enables organizations to move forward pragmatically while building the organizational capabilities required to scale compliance across large product portfolios.

For organizations developing advanced digital technologies, including AI-enabled systems, aligning cybersecurity with broader trust and compliance frameworks is becoming increasingly important. Building these capabilities today allows companies to meet CRA obligations while delivering digital products that are secure, resilient, and trustworthy by design.

At Nemko Digital, we are able to support a substantial part of the CRA preparation effort, covering up to around 80% of the required activities. This is especially valuable for organizations with limited internal capacity or complex product portfolios. We provide end-to-end support across governance, risk assessment, implementation, and compliance preparation within the broader cybersecurity domain, helping organizations translate CRA requirements into operational practices in a structured and scalable way.

About the author



Alicja Halbryt

Before joining Nemko Digital, Alicja Halbryt worked for the Dutch Ministry of Economic Affairs as an AI standardisation expert at CEN/CENELEC JTC 21. She holds an MSc in Philosophy of Technology and an MA in Human-Centred Design. She is dedicated to shaping an ethical and human-aligned AI ecosystem.

Nemko Digital