ATHENE
National Research Center
for Applied Cybersecurity

Cyber Resilience Act
Risk Management

Recommendations for the Implementation of Risk Management under the CRA

Steven Arzt
George Gkoktsis
Michael Kreutzer
Kirstin Scheel
Linda Schreiber
Hervais Simo Fhom

Version 1.0
July 2025

EDITH GERMANY
Enabling Digital Innovation & Technology in Hesse

Cyber Resilience Act
Risk Management

Recommendations for the Implementation of Risk Management under the CRA

Publishing Notes and Contact:
National Research Center for Applied Cybersecurity ATHENE
c/o Fraunhofer Institute for Secure Information Technology SIT
Rheinstrasse 75
64295 Darmstadt, Germany

Authors
Steven Arzt
George Gkoktsis
Michael Kreutzer
Kirstin Scheel
Linda Schreiber
Hervais Simo Fhom

Funding Acknowledgements
This paper was supported with funds from the German Federal Ministry of Research, Technology and Space (BMFTR) and the Hessian Ministry of Science and Research, Arts and Culture (HMWK) as part of their joint funding for the National Research Center for Applied Cybersecurity ATHENE.

Its preparation was also supported by the BMFTR project StartupSecure and by funds provided by the European Digital Innovation Hub EDITH, which receives financing as part of the European Commission's Digital Europe Programme.

Disclaimer
The information contained in this paper was drafted carefully but is not a substitute for legal advice. The authors and publishers therefore make no warranty, express or implied, that this information meets the specifications of the current legal situation.

The same applies to the usability and completeness of the information and to its being free of errors, with the result that any and all liability for damage and/or losses that may arise from the use of this work product / information is expressly disclaimed. This disclaimer does not apply in cases of intentional acts.

Download
You can download the latest version of this article at:
https://www.athene-center.de/cra

Content

Overview and Intended Readership

The EU Cyber Resilience Act (CRA)[1] entered into force on December 10, 2024. Following an implementation period of 21 or 36 months, standardized cross-sector and cross-area requirements for the cybersecurity of connected hardware and software products will then apply Europe-wide. The comprehensive regulatory approach created by the CRA will apply cybersecurity rules for the first time to many companies that were not covered by existing product-specific, consumer-specific, or sector-specific regulations.

This white paper provides an analysis of cybersecurity risk management within the framework of the CRA, offering both conceptual insights and practical implementation guidance for manufacturers of products with digital elements.

The CRA represents a significant shift in the European regulatory landscape, establishing mandatory cybersecurity requirements for products with digital elements throughout their entire lifecycle. At its core, the regulation adopts a product-centric approach to cybersecurity risk, focusing on ensuring that digital products entering the EU market are designed, developed, and maintained with robust security measures.

Since the CRA introduces horizontal cybersecurity requirements and thereby covers a broad range of products and product categories, it relies on a risk-driven approach to instantiate concrete cybersecurity measures. Manufacturers must assess and monitor the cybersecurity risks associated with their products. Although all products are bound by the essential requirements described in Annex I CRA, the risk model defines how these high-level measures flow down to the product at hand. Depending on the risks, the concrete measures, e.g., for protecting the confidentiality of data, may differ significantly between industrial production machines or smart home devices.

Our analysis highlights that the CRA's approach to cybersecurity risk differs from traditional frameworks by emphasizing product-level risks rather than organizational security postures. While established standards like ISO/IEC 27001 and other legislation such as the EU NIS-2 Directive[2] focus on protecting organizational assets (including processes) and infrastructure, the CRA places responsibility on product manufacturers to implement security-by-design principles and continuous vulnerability management processes.

1 Published in the Official Journal of the European Union under its full title "Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements".

2 Published in the Official Journal of the European Union under its full title "Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union".

The white paper details the specific risk management obligations under the CRA as well as the duties that arise from the need to mitigate these risks. This includes conducting continuous risk assessments, implementing secure development practices, managing vulnerabilities, providing timely security updates, maintaining comprehensive technical documentation, and demonstrating compliance through conformity assessment procedures. These requirements apply throughout the product lifecycle, from initial design to post-market support.

For practical implementation, we provide a structured methodology for integrating CRA risk management requirements into Secure Development and Operations (SecDevOps) processes, with specific guidance for each development phase. Our approach maps CRA obligations to concrete technical controls and tools, enabling manufacturers to embed security considerations throughout their development workflows.

This white paper is based on the current status of documents published by official bodies at the time of publication. The recommendations in this document are provisional, subject to future publications by official bodies that concretise the requirements of the CRA. Updated versions of this white paper may be published in the future and will be made available at https://www.athene-center.de/cra.

By adopting the methodologies presented in this white paper, manufacturers can not only address CRA requirements but also enhance their overall product security posture, reduce incident response times, and establish a competitive advantage through demonstrable security practices that build customer trust. This white paper is thus intended for those at the intersection of compliance, IT, risk management, and general management – depending on who within the organization oversees the processes analyzed herein.

The ATHENE website (https://www.athene-center.de/cra) provides information on events, contacts, and comprehensive resources related to the Cyber Resilience Act, including the latest versions of two white papers – one focused on the legal requirements of the CRA and the other on its technical aspects.

Part 1

Risk Management Fundamentals and the CRA

This chapter introduces the fundamentals of cybersecurity risk management in the context of the EU Cyber Resilience Act (CRA). It begins with a brief introduction to cybersecurity risks, explaining how they are conceptualised and managed under the CRA. It then provides an in-depth analysis of the CRA's specific provisions and requirements on cybersecurity risks. Finally, the chapter emphasises the innovative focus of the CRA and its implications for organisations operating in the EU single market by highlighting the unique characteristics that distinguish risk under the CRA from traditional cybersecurity risk frameworks.

At a Glance: Nature of Cybersecurity Risk and Risk in the Spirit of CRA

In traditional risk assessment (safety risks, business risks, etc.), the term "risk" refers to the potential occurrence of unfavourable outcomes resulting from uncertainty. It is generally characterized primarily by two factors: the likelihood (probability) of an adverse event occurring and the magnitude (severity) of its potential consequences, such as loss, disruption, damage, or harm. In essence, risk combines uncertainty about future events with their potential negative impacts, guiding decision-making in mitigating or managing such uncertainties.

In contrast, cybersecurity risk refers to the potential for harm, loss, or disruption arising from wilful actions of an adversary against IT systems and digital assets. These undesirable consequences may be intended by the attacker or may be collateral damage from an attack. The cybersecurity risk notion encompasses threats to both digital and non-digital assets that are accessible through or reliant on cyberspace. This form of risk is typically associated with breaches of confidentiality, integrity, or availability due to vulnerabilities in connected hardware and software, malicious actors (internal or external), or human error that degrades security, e.g., through misuse or misconfiguration. As such, cybersecurity risks exist at the intersection of technical vulnerabilities and evolving threats within interconnected digital environments.

The CRA is a legal framework designed to ensure that products with digital elements made available on the EU market are designed, developed, and maintained with a high standard of cybersecurity throughout their lifecycle – from initial design to deployment and post-market support. The CRA applies broadly to both software and hardware. Within the context of the CRA, cybersecurity risk specifically refers to risks associated with a product with digital elements and means the potential for loss or disruption caused by an incident.

By addressing these risks, the CRA aims to reduce the likelihood and impact of cybersecurity-related incidents and enhance the overall resilience of the digital ecosystem. This approach safeguards the interests of EU citizens and businesses and fosters a more secure digital environment across the Union. The CRA mandates that product manufacturers implement and maintain effective processes for identifying, assessing, and mitigating cybersecurity risks and vulnerabilities stemming from

their products' reliance on digital components and cyber artefacts. Manufacturers must also provide adequate information and instruction to users that considers and reflects, among other things, the product's intended purpose, as well as any known or foreseeable circumstances that may lead to significant cybersecurity risks during intended use or reasonably foreseeable misuse.

The following requirements and processes for cybersecurity risk management are of particular importance under the CRA:

1. **Continuous risk assessments.**
   Manufacturers are required to update risk assessments appropriately throughout the product's support period. These assessments should identify cybersecurity risks associated with the product and its dependencies, enabling manufacturers to estimate and update the likelihood and severity of impact of a potential threat event (i.e., an event emerging from the exploitation of a cybersecurity vulnerability).

2. **Implementation of secure development practices, encompassing both security-by-design and security-by-default methodologies, is imperative.**
   Products with digital elements must be engineered in ways that proactively minimize risks and reduce the likelihood and impact of incidents from the outset.

3. **Management of both known and emerging vulnerabilities.**
   Manufacturers must establish robust vulnerability handling processes, including mechanisms for detecting, documenting, reporting, and remediating cybersecurity vulnerabilities in a timely manner. Adhering to coordinated vulnerability disclosure practices is crucial for being informed about vulnerabilities, but also for transparency and rapid response.

4. **Prompt release of security updates.**
   To ensure rapid mitigation of cybersecurity threats, the CRA requires manufacturers to address and remediate vulnerabilities without delay, e.g., by distributing security patches. The CRA further mandates that security updates must be free of charge and thereby not forcing the customer to purchase a new product, ensuring the security of legacy systems athroughout their lifetime.

5. **Ensure transparency and maintain technical documentation.**
   Manufacturers must draw up comprehensive technical documentation prior to placing products on the market and make this documentation available upon request of the market surveillance authorities. The technical documentation includes e.g., details on the product's cybersecurity features, its intended purpose, the assessment of the cybersecurity risks and where applicable a Software Bill of Materials (SBOM). The documentation must be maintained and updated throughout the product support period to ensure ongoing compliance. To support informed decision making by users, manufacturers also must ensure that products are accompanied by information and instructions to the user that encompass e.g., the product's intended purpose and circumstances which may lead to cybersecurity risks, the duration and type of technical security support provided, detailed instructions for secure installation and configuration, and guidance on security update installation procedures.

6. **Demonstration of compliance through conformity assessment.**
   Manufacturers are required to demonstrate compliance with the CRA. This involves subjecting the product to a conformity assessment to demonstrate that the product meets all applicable cybersecurity requirements set out in the CRA before placing it on the EU market. Successful assessment confirms that the product adheres to the essential cybersecurity requirements necessary for market access within the European Union.

As such, managing cybersecurity risk under the CRA is not merely reactive, but also proactive and continuous. Robust cybersecurity design processes must be considered to ensure that products meet stringent security requirements, safeguard consumers, and protect the broader European digital ecosystem from cyber threats.

In Depth: Analysis of the CRA Risk-Related Provisions and Requirements

How is the assessment of cybersecurity risks included in the CRA?

The assessment of cybersecurity risks is central to the obligations that arise for manufacturers of products with digital elements under the CRA. Annex I Part I (1) CRA states that:

> *"Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."*

This fundamental rule is further elaborated in the context of the specific obligations for manufacturers in Art. 13 (2) CRA. Manufacturers are therefore obliged to carry out an assessment of cybersecurity risks associated with a product, and take the outcome into account in all phases of the product's life cycle from planning, design and development to production, delivery, and maintenance to minimize cybersecurity risks, prevent incidents and minimize their impact, including in relation to the health and safety of users.

Cybersecurity risk is generally defined in Art. 3 (37) CRA as "the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident".

Further requirements and parameters for the cybersecurity risk assessment are set out in Art. 13 (3) CRA and include:

- Documentation of the cybersecurity risk assessment
- Updating cybersecurity risk assessment during support period (as appropriate)
- Assessment shall comprise at least an analysis of cybersecurity risks based on the products:
  - intended purpose (use intended by the manufacturer such as context and conditions of use as specified in information material supplied by the manufacturer, Art. 3 (23) CRA)
  - reasonably foreseeable use (not necessarily intended use but which is likely to result from reasonably foreseeable human behaviour, technical operations or interactions, Art. 3 (24) CRA)
  - conditions of use (such as operational environment or assets to be protected)
  - expected length of time to be in use

A further central component of the CRA and the obligations for manufacturers of products with digital elements is the list of essential cybersecurity requirements relating to the properties of a product set out in Annex I Part I (2) CRA. These requirements must be fulfilled on the basis of the risk assessment and include, for example, that a product is made available on the market without known exploitable

vulnerabilities (a) or has limited attack surfaces (j). Furthermore, Annex I Part II CRA contains requirements for manufacturers for the handling of vulnerabilities, for example remediating vulnerabilities e.g., through security updates (2), regular tests and reviews of the security of a product (3) or putting in place and enforcing a policy for coordinated vulnerability disclosure (5).

A mandatory component of the risk assessment under the CRA is to indicate whether and, if so, how the cybersecurity requirements are applicable for the respective product and how these requirements are implemented based on the cybersecurity risk assessment. The risk assessment should also specify how vulnerability handling requirements and the general requirement to design, develop and produce products in a way that an appropriate level of cybersecurity based on the risks is ensured are applied (Art. 13 (3) CRA).

Aligning with the New Legislative Framework (NLF) approach[3], manufacturers must demonstrate conformity with the cybersecurity requirements and risk assessment obligations under the CRA by, in particular, performing appropriate conformity assessment procedures (Art. 32, Annex VIII CRA). The type of procedure required depends on the product's classification. Products with digital elements that have certain functionalities may be classified as "important products with digital elements" (Class I and II listed in Annex III CRA), and "critical products" (listed in Annex IV CRA). For products with digital elements that do not fall in these categories, manufacturers may apply a conformity assessment procedure that does not involve an external third-party (internal control). Important and critical products with digital elements require stricter procedures that might involve notified bodies as independent third-party entities.

Furthermore, the CRA incorporates harmonized standards and European cybersecurity certificates as a key element in the conformity assessment process (Art. 27 CRA). Products that comply with harmonized standards (or parts thereof) published in the Official Journal of the European Union are presumed to be in conformity with the corresponding cybersecurity requirements. Additionally, conformity with cybersecurity certification schemes under the Cybersecurity Act (Regulation (EU) 2019/881) may be recognized as demonstrating compliance with CRA requirements if specified by the European Commission. This standards-based approach provides manufacturers with technical guidance for implementation and simplifies the conformity assessment by creating a "presumption of conformity," which reduces the burden of proof on manufacturers who follow these standards.

Spotlight: How is Risk in the CRA different from other Cybersecurity Risks?

Risk is a central concept in all widely recognized international cybersecurity standards and frameworks. However, its interpretation and practical implementation varies depending on the legal context, the specific characteristics of the target systems and the size and role of the actors involved. Even if the wording of the regulation and the jargon used in the CRA conforms to cybersecurity phraseology, there is indeed a conceptual difference that makes a substantial impact on how we approach CRA related risk assessment. This difference is that the risks, and by extension the protection mechanisms relating to the risks, refer to the recipient of the product with digital elements, instead of the entity assessing and mitigating the product. Moreover, this divergence also arises from the CRA's product-centric focus, which contrasts with the organization- and infrastructure-oriented perspectives of most other cybersecurity standards.

3 More detailed information on this subject can be found in the legal ATHENE white paper on the CRA: https://www.athene-center.de/cra

To highlight this distinction clearly, we will examine how cybersecurity risk is approached by state-of-the-art cybersecurity standards as well as established legislation and contrast this approach with the concept of risk as defined in the CRA. Table 1 provides a comparative summary of the key differences between the CRA's understanding of cybersecurity risk and the approaches adopted in established practices, frameworks and standards such as the NIS-2 Directive, ISO/IEC 27001; ISO/IEC 27002, ISO/IEC 27701, ETSI TR 103305 and those issued by the BSI, e.g., BSI 200-x.

Aspect	CRA	Established good practices and standards*
Focus of Risk Management	Product-centric (individual product with digital elements)	Organization- and infrastructure-centric
Primary Objective	Ensure cybersecurity in relation to products throughout lifetime	Protect organizational assets, services, and infrastructure
Primary Responsibility	Manufacturers of products placed on the EU market	Organisations of various sizes and sectors
Risk Assessment Frequency	Updated as appropriate during support period	Sufficiently short regular intervals or in response to significant changes
Documentation Requirements	Detailed technical documentation, SBOM and additional information and instructions to the user	General risk management and security policy documentation
Views on Supply Chain	Indirectly addresses supply chain risk via requirements for SBOMs, secure update mechanisms, categorisation as critical product, mandates of national and EU-level authorities regarding products representing a significant cybersecurity risk	Explicitly address supply chain risk (e.g., ISO/IEC 27036-3, Art. 21 NIS-2 Directive). Require assessment and management of third-party suppliers' security posture. Define risk in terms of dependency and trust relationships.
Compliance Goal	Prerequisite for EU market access	Security maturity and resilience (e.g., NIS-2 Directive)
Compliance Mechanism	Mandatory conformity assessment/ mechanisms for presumption of conformity and CE marking before market access	Self-assessment, third-party audits, or regulatory oversight

** (e.g., NIS-2 Directive, ISO/IEC (27001; 27002; 27701), ETSI TR 103 305, BSI IT-Grundschutz)*
Table 1. Aspect of Cybersecurity risk - CRA vs. Established cybersecurity legislation and standards

Notion and Scope of Cybersecurity Risk. At the core of the CRA lies a product-centric understanding of cybersecurity risk. Risk is assessed in terms of the potential for loss or disruption caused by an incident associated with a particular product with digital elements, which may include software, hardware or integrated IoT devices. The CRA requires that risk must be assessed and addressed throughout the product lifecycle - from design and development through to distribution, use and support. In contrast, state-of-the-art cybersecurity standards such as ISO/IEC 27005 (Risk Management) and the BSI IT-Grundschutz Compendium adopt a broader, systems- or organization-based view of risk. This approach is operational and strategic (i.e., rooted in the organisation's security strategy, focusing on business continuity, data protection, user access control, and IT governance) and not limited to the characteristics of individual products.

Views on supply chain risks. The CRA indirectly addresses supply chain risks through requirements for SBOMs, secure update mechanisms, through the categorisation of products with digital elements as critical and the mandates of national and EU-level authorities regarding products that represent significant cybersecurity risks. These measures aim to enhance product transparency and traceability. In comparison, established frameworks like ISO/IEC 27036-3 and NIS-2 Directive (Art. 21) take a more expansive view. They define supply chain risk in terms of dependency and trust, requiring active oversight of external entities (e.g., third-party suppliers) that may affect security. The CRA, by contrast, is more narrowly focused on ensuring transparency in the product supply chain rather than managing trust-based dependencies on an organizational level.

Risk management responsibility. Under the CRA, the primary responsibility for managing cybersecurity risk rests with product manufacturers (secondarily with importers and distributors). Manufacturers must ensure that their products are secure by design and secure by default, taking into account foreseeable misuses and deployment in complex networked environments. In addition, manufacturers are also required to handle vulnerability disclosures, provide timely updates, and assist users in maintaining secure configurations. Conversely, standards like ISO/IEC 27001 or the NIS-2 Directive assign risk management responsibilities to operators of critical services or information systems. These operators must implement organisational and technical measures (e.g., access control mechanisms, incident response and staff training) to manage operational risks, including those stemming from third-party components regulated under the CRA.

Lifecycle vs. operational risk management. The CRA integrates risk management explicitly into the product lifecycle. It requires manufacturers to implement: 1) Secure design and development practices; 2) Secure default settings and a secure manufacturing process; 3) Continuous monitoring and timely updates; and 4) Creating a SBOM to aid third-party risk assessment. This preventative, lifecycle-focused approach contrasts with frameworks like ISO/IEC 27001, which emphasise ongoing operational risk management through security management systems for deployed infrastructures and networks. The CRA targets upstream risks at the product level, while traditional frameworks concentrate on securing operational environments post-deployment.

Risk management objectives (compliance and resilience). Another key distinction lies in the objective of risk management. Under the CRA, manufacturers must demonstrate conformity - potentially through third-party assessment procedures, especially for critical products - before market entry. In contrast, state-of-the-art standards such as ISO/IEC 27001, are typically regarded as voluntary frameworks unless stipulated in regulatory (e.g., NIS-2 Directive) and contractual settings. These standards are designed to enhance an organisation's overall resilience to cyber threats. Organisations are obligated to maintain risk management protocols and may be subject to audits; however, the individual products themselves are not necessarily subjected to testing.

In essence, while the CRA's view of cybersecurity risk differs significantly from that of well-established cybersecurity frameworks and standards, it is complementary rather than contradictory. Indeed, CRA promotes security-by-design and secure-by-default principles, focusing on mitigating risks at the product level. In contrast, traditional standards promote secure-by-operation, embedding risk management within broader organisational strategies. As such, CRA fills a critical gap in the cybersecurity landscape by shifting risk management upstream to the product level and reinforcing downstream efforts that focused on systemic resilience and operational governance across the entire organization's digital ecosystem.

Part 2

Step-by-Step Guide to CRA Risk Management

This chapter provides a practical, structured guide to meeting the cybersecurity risk management requirements of the Cyber Resilience Act (CRA). It starts by outlining a clear, step-by-step overview of the cybersecurity risk management process. Next, the chapter delves into how manufacturers can effectively integrate the CRA's requirements into their Secure Development and Operations (SecDevOps) processes. Finally, the chapter spotlights engineering good practices for translating CRA cybersecurity risk obligations into actionable technical requirements, enabling robust, systematic compliance.

At a Glance: The Process of Cybersecurity Risk Management

Operating any business inherently involves accepting a certain degree of risk. However, organisations in both the public and private sectors need, on the one hand, to develop a better understanding of cybersecurity risk in the broader context of risk management as well as in relation to their organisational operations and assets. On the other hand, organisational leaders remain responsible for managing risk, particularly the risks that arise from operating and relying on IT systems that are essential to their mission and business functions. As such, risk management should be viewed not as a siloed function, but as a core management function that spans all areas of the organization and should ideally be executed in a coherent and integrated manner.

The general risk management process typically consists of four distinct steps, starting with "risk framing", a step in which assumptions about the environment in which the organisation intends to manage risk are specified and a risk management strategy is developed. This is followed by an assessment of the same so probability and impact can be taken into account. Once this has been done, potential mitigation measures (i.e., means to reduce likelihood and impact), are evaluated and the level of residual risk estimated. Depending on the outcome of such an assessment, organisations may need to introduce further measures and restart the assessment. The final step, risk monitoring, involves ongoing reassessment of the effectiveness of risk response measures and reconsideration of the initial/current risk framing and risk assessment. This process will go through several iterations until the residual risk has decreased to acceptable levels – or the underlying principles have changed, and the risk assessments needs to be re-done.

The approach to risk management is shaped by the structure and size of an organisation, the complexity of its information systems, the nature of its business and the underlying regulatory environment. In addition, legal and other compliance requirements need to be considered when choosing the right risk management framework. Understanding and setting the correct context, including regulatory, economic, and industry factors, will influence the approach as much as the necessity to involve stakeholders at all levels of corporate existence to create a comprehensive review of all risks to the organization. However, organizations have considerable flexibility in carrying out risk management processes, for example in the level of detail and formality applied and the overall depth of analysis. Organisations also have control over how the results of the risk management process are communicated, both internally and externally.

At this juncture it should be mentioned that ENISA has published numerous tools to help implement an EU cyber risk management framework. This includes amongst others a "Compendium of Risk Management Frameworks with Potential Interoperability"[4] as well as a "Interoperable EU Risk Management Toolbox"[5]. Both give a broad overview of approaches and established frameworks that will help standardize an organization's approach. The overall goal is to create European interoperability as cybersecurity is a pan-European challenge.

In Depth: How to Integrate the CRA Risk Management Requirements into your SecDevOps

As described above, the CRA does not introduce fundamentally new principles, but rather codifies and harmonizes good practices in part from existing cybersecurity standards and frameworks, aiming for consistent implementation of cybersecurity policies across EU markets.

Integrating the risk management requirements from the CRA into a SecDevOps process means embedding risk management activities and cybersecurity controls directly into the DevOps pipeline. This means in turn ensuring that CRA obligations are continuously addressed as part of product development, operations and maintenance.

CRA Risk Requirement	SecDevOps Phase	Supporting Mechanisms
Threat/Risk Identification	Plan / Design	Threat modelling, risk assessment tools (e.g., OWASP Threat Dragon, STRIDE, MITRE ATT&CK, Space Shield, …)
Security-by-Design & Default	Design / Implement	Security requirements, secure/security libraries (e.g., derived from risk models)
Vulnerability Management	Build / Test / Deploy / Operate	SAST, DAST, SCA, container scanning, patch management, dependency management (e.g., CodeQL, VUSC, OWASP Dependency Scan, …)
Security Validation & Testing	Test	Automated security testing, manual penetration testing (e.g., Nikto, SQLmap, …)
Documentation & Traceability	All phases	Secure Development Lifecycle artifact management, SBOM generation, logging (e.g., CycloneDX, SPDX, …)
Conformity & Compliance Checks	Release / Operate	Compliance-as-code, policy-as-code, infrastructure-as-code

Table 2. Mapping CRA Requirements to SecDevOps phases

4 https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Compendium%20of%20Risk%20Management%20Frameworks%20with%20Potential%20Interoperability.pdf, last checked 30.06.2025

5 https://www.enisa.europa.eu/sites/default/files/publications/Interoperable%20EU%20RM%20Toolbox.pdf, last checked 30.06.2025

When integrating CRA Risk Management requirements into SecDevOps, we recommend focusing on the following key stages of SecDevOps in particular. A mapping of CRA requirements to typical SecDevOps phases is provided in Table 2.

- During the initial phase, i.e., **planning and design phase**, threat modelling must be conducted early to identify potential cybersecurity risks relevant to the product's digital context and intended use cases as well as to design for the required security measures right from the start. This proactive risk identification aligns with CRA requirements for continuous and lifecycle-spanning risk management. To assess the security posture of the product's components and data flows, developers can rely on tools such as OWASP Threat Dragon or the Microsoft Threat Modelling Tool. These tools provide visual interfaces and modelling frameworks. Established methodologies such as STRIDE, DREAD or LINDDUN can be utilised to structure this process even more effectively. These tools and methodologies also facilitate the categorisation of threats by type of impact, likelihood or privacy concerns, in accordance with the CRA requirement for a proactive risk identification process. All risks identified at this stage are logged in a dedicated risk register. This register should be maintained within a secure documentation system. This facilitates the tracking of affected components, the recording of mitigation actions/strategies, and the maintenance of traceability throughout the product's lifecycle. Furthermore, non-functional security requirements derived from CRA obligation (see e.g., Annex I CRA) must also be considered at this stage. These include aspects such as the need to minimise the attack surface of the product at hand, secure default configurations, and mechanisms for updates and patches.

- In the **development and coding stage**, secure coding practices should be strictly enforced. Developers must follow guidelines that align with Common Weakness Enumeration (CWE) classifications, thereby ensuring the resilience of code to prevalent common vulnerabilities such as buffer overflows or command/SQL injections. Static application security testing (SAST) tools such as e.g., SonarQube, Checkmarx or VUSC[6] should be fully integrated into the continuous integration (CI) pipeline. These tools allow for automated code scans at every commit or merge, enabling early detection of security flaws before the application advances to the build phase. Furthermore, it is imperative that supply chain security is addressed through the utilisation of Software Composition Analysis (SCA). Indeed, tools such as Dependency-Track or Snyk should be used to detect vulnerabilities in open-source dependencies and libraries. Tools such as these also facilitate the generation and maintenance of a Software Bill of Materials in relevant formats, e.g., SPDX or CycloneDX, which is a critical requirement under the CRA to ensure product transparency and supply chain traceability. To promote security-by-design/-default behaviour further, developers should regularly receive training and be supported with practical code examples, secure design checklists, and structured peer review processes.

- In the **build and packaging phase**, container images and build artefacts should be scanned for known vulnerabilities and misconfigurations. Tools such as e.g., Docker Scout and Trivy could be integrated into the pipeline to detect security weaknesses prior to deployment. Ensuring the integrity of the build environment is critical to preventing unauthorized interference and maintaining a secure development process. This can be achieved by relying on measures such as the isolation of CI/CD runners, strict control of environment variables, and enforcement of robust access controls. Cryptographic signatures should be used to guarantee the authenticity and integrity of build artefacts.

- **During the testing phase**, the scope of security testing should extend well beyond conventional unit and integration testing. Dynamic Application Security Testing (DAST) tools such as OWASP ZAP or Nikto should be executed within

6 VUSC – der Codescanner https://www.sit.fraunhofer.de/de/vusc/

staging environments or integrated directly into test pipelines to simulate external attacks on running applications. Fuzz testing tools such as libFuzzer and OSS-Fuzz can be used to automatically discover issues such as memory corruption and logic flaws. Compliance validation should also be automated by integrating tools such as KICS or Checkov, which analyze Infrastructure as Code (IaC) files for misconfigurations and security policy violations. Furthermore, policy enforcement could also be carried out, leveraging frameworks like Open Policy Agent (OPA) to ensure that deployment configurations adhere to CRA-aligned security requirements.

- In the **release and deployment stage**, configuration hardening must be enforced by applying secure defaults and limiting open ports, services, and privileges using Infrastructure as Code templates. More specifically, it is imperative that products support secure over-the-air (OTA) update mechanisms by default that incorporate rollback capabilities and digital signature verification for update packages. This guarantees that updates down the line are both authentic and secure, a prerequisite for the provision of long-term product support as outlined in the CRA. Furthermore, it is crucial that release artefacts and container images are signed prior to distribution, employing trusted key management and signature verification tools such as GNU Privacy Guard (GPG), Sigstore's cosign or AuthentiCode on Windows.
- Finally, in the **operations and monitoring phase**, continuous security monitoring and observability are essential. The collection, parsing and analysis of targeted logs from applications, such as anonymized crash reports, should be conducted in cooperation with distributors. This approach facilitates timely threat detection and post-incident analysis.

(!) A **Coordinated Vulnerability Disclosure (CVD)** process, supplementary to internal testing processes, leveraging established procedural guidelines is vital to ensure that details about discovered cybersecurity vulnerabilities are responsibly communicated, managed, and remediated. Specifically, a wellstructured CVD process aims is to facilitate clear communication and coordinated action between vulnerability finders (such as security researchers), product manufacturers/vendors, and other affected stakeholders (e.g., users, third parties and the broader public). To comply with the provisions of the CRA, organisations have to establish a designated single point of contact where information about vulnerabilities can be reported and received as well as the CVD policy can be found. According to the CRA, all related technical documentation, test results, vulnerability scan logs, SBOMs, risk registers, and compliance artefacts need to be machine-readable. Such documentation is critical and must be versioned and stored securely, enabling traceability of security decisions, configurations, and changes. As part of an automated risk-based approach, continuous risk assessment must be conducted. Scoring frameworks, such as, or similar to, CVSS, or custom metrics that combine threat likelihood, potential impact, and exploit maturity might be utilized to as risk monitoring approaches. Such scores are then utilised to inform automated decision gates embedded within CI/CD pipelines. For example, a pipeline may automatically reject a deployment if critical vulnerabilities are detected in a container image or if an SBOM indicates the use of outdated or unpatched dependencies. Risk dashboards might aggregate these scores to provide real-time visibility to product owners, compliance managers, and security teams, enabling faster, evidence-based decision-making.

By embedding cybersecurity risk management into every phase of the SecDevOps workflow, manufacturers not only meet CRA obligations but also enhance their overall product security posture. Furthermore, such an integration can also result in a reduction in incident response times and the establishment of a long-term competitive advantage through demonstrable compliance and strengthened customer trust.

Spotlight: How to Engineer the CRA Cybersecurity Risk Requirements

To systematically and rigorously implement the requirements of the Cyber Resilience Act, product manufacturers must adopt a formal, well-defined engineering process. This process is one that translates abstract regulatory statements into actionable technical requirements and specifications. These requirements and specifications span the entire product lifecycle and pertain to architectural design, software development practices, operational procedures, and post-market activities such as security updates and vulnerability management. From a technical standpoint, various requirements engineering frameworks exist, to aid in this endeavour. These include the NIST Risk Management Framework (SP 800-160 Vol. 1 and 2), the ISO/IEC 27001–27005–62443 suite, the OWASP Software Assurance Maturity Model (SAMM), the MITRE Systems Engineering Guide and ATT&CK framework (especially relevant to Art. 11 CRA, where the General Product Safety Regulation provisions are mentioned), and the Scaled Agile Framework (SAFe). Each of these frameworks has its strengths and weaknesses and is in varying degrees of alignment with the CRA requirements. In this section, we will briefly describe two of these methodologies and subsequently overview their larger landscape.

Arguably the most rigorous methodology for this purpose was developed by the International Council on Systems Engineering (INCOSE)[7]. The INCOSE requirements engineering process provides a comprehensive framework that has been crafted to navigate the complexities inherent in development of digital products. It ensures that stakeholder needs are not merely acknowledged but comprehensively integrated into the entire lifecycle of IT systems (products in CRA context). Characterized by its iterative and structured nature, the INCOSE process unfolds through a series of interconnected phases that, collectively enhance the robustness of system requirements. The INCOSE approach to requirements engineering includes five key activities:

1) requirements elicitation from stakeholders;
2) requirements analysis and refinement;
3) requirements specification (clear, testable, and traceable);
4) requirements validation & verification;
5) Lifecycle integration.

However, this rigor comes at a cost: the method can be quite heavyweight, demanding extensive upfront documentation, formal reviews, and well-defined artifacts, which may slow down rapid, agile development cycles and offer limited practical guidance on translating high-level regulatory mandates (like the CRA) into granular, developer-level tasks.

7 INCOSE Guide to Writing Requirements: https://www.incose.org/docs/default-source/working-groups/requirements-wg/gtwr/incose_rwg_gtwr_v4_040423_final_drafts.pdf?sfvrsn=5c877fc7_2, last checked 30.06.2025

On the other hand, more SecDevOps-friendly methods exist. The OWASP SAMM, for instance, is a lightweight, iterative framework for embedding security throughout the software lifecycle. It is organized into Governance, Design, Implementation, Verification, and Operations domains, each comprising defined activities and maturity levels. Under this scheme, CRA requirements forsecurity by design and by default principles, vulnerability management, and secure update mechanisms, would be mapped to SAMM practices (e.g., Threat Assessment, Security Requirements, Secure Build, Security Testing), thereby translating legal mandates into developer-oriented tasks, for example, security user stories, SAST/DAST integration, vulnerability-disclosure workflow, and tracking progress via the SAMM improvement roadmap. However, because SAMM is structured as a maturity model rather than a prescriptive control catalogue, concrete technical requirements and test cases are not provided and must be derived from supplementary sources, such as OWASP ASVS, and its high-level focus and requirement for ongoing metric tracking may render it challenging to implement within small, fast-paced teams for secure development.

Table 3 provides a synoptic overview of these methodologies, comparing their areas of emphasis, compatibility with the CRA, and specific limitations and strengths in addressing cybersecurity requirements.

Methodology / Framework	Primary Focus	CRA Alignment	Strengths	Limitations
INCOSE Requirements Engineering	Systems engineering and structured RE process	High. Comprehensive lifecycle traceability and formal specification	Rigorous lifecycle coverage, traceability, stakeholder alignment	May require tailoring for agile/SecDevOps settings; heavyweight for fast-paced environments
NIST SP 800-160 Vol. 1 & 2	Systems Security Engineering	Very High. Directly addresses secure-by-design principles mandated by CRA	Deep security engineering principles, integrates with NIST RMF, aligns with lifecycle resilience; widely adopted	Can be complex; assumes mature engineering processes
ISO/IEC 27001, 27005, 62443-4-1/2	Risk-based information and industrial security	High. Structured support for secure development lifecycle (SDLC)	Internationally recognized standards; maturity models; supply chain focus (62443); certifiable	Requires institutional process integration; partial coverage of agile pipelines
OWASP SAMM	Secure software development maturity	Medium to High. Aligns well with CRA software process requirements	Developer-centric; incremental adoption; actionable maturity goals; lightweight, developer-friendly	Less system-level focus; less coverage of physical product/ embedded context
MITRE ATT&CK / D3FEND + Systems Engineering Guide	Threat-informed defense and mitigation mapping	High. Particularly relevant for vulnerability management	Grounded in real-world threats; supports control mapping and testable requirements; adversary-focused	Reactive posture if used alone; needs integration with RE processes
STPA-Sec (System-Theoretic Process Analysis – Security)	Safety and control-based security requirements	Medium to High. Translates systemic hazards into security constraints	Handles complex interdependencies; strong on architectural-level reasoning	Less known in industry; needs expert facilitation
SQUARE Methodology (CMU SEI)	Security Requirements Engineering	High. Especially suitable for translating regulatory language into concrete requirements	Lightweight but structured; bridges legal-to-technical translation gap	Best in early stages; not focused on continuous delivery
Scaled Agile Framework (SAFe)	Agile security integration at enterprise scale	Medium. Supports integration of security in iterative delivery	Aligns security with agile delivery cycles; supports Secure Development Lifecycle (SDLC)	Needs customization to enforce regulatory alignment and documentation rigor

Table 3. Comparative Analysis of (Selected) Methodologies for Security Requirement Analysis

Conclusions

The Cyber Resilience Act represents a paradigm shift in the European regulatory approach to cybersecurity, moving from primarily organization-focused to product-centric risk management.

Key takeaways from our analysis include:

1. The CRA establishes a comprehensive framework for managing cybersecurity risks in products with digital elements, requiring manufacturers to adopt security-by-design principles, implement continuous vulnerability management, and provide transparent information to enhance the overall security posture of digital products in the EU market.

2. While the CRA's approach differs from established cybersecurity legislation and standards, it creates a synergistic relationship between product-level security (regulated by CRA) and organizational security management (covered by standards and legislation like ISO/IEC 27001 and NIS-2), resulting in a more robust digital ecosystem.

3. Effective implementation of CRA requirements necessitates their integration into every phase of the development lifecycle, from planning and design through deployment and operations, requiring a structured approach to requirements engineering and security controls.

4. The mapping of CRA obligations to SecDevOps processes provides manufacturers with a practical pathway to compliance while enhancing overall product security, potentially reducing security incidents and associated costs in the long term.

5. Going beyond mere compliance, organizations that effectively implement CRA requirements can gain competitive advantages through improved product quality, enhanced customer trust, and reduced security-related liabilities.

As the digital landscape continues to evolve with increasing interconnectivity and complexity, the CRA establishes a foundation for a more secure digital environment across the European Union. By requiring manufacturers to take responsibility for the security of their products from inception through support, the legislation aims to reduce the cybersecurity burden on end-users and organizations while raising the baseline security level of digital products. Organizations that view CRA compliance not as a regulatory hurdle but as an opportunity to enhance their security practices will be better positioned to succeed in an increasingly security-conscious market.

ATHENE
National Research Center
for Applied Cybersecurity