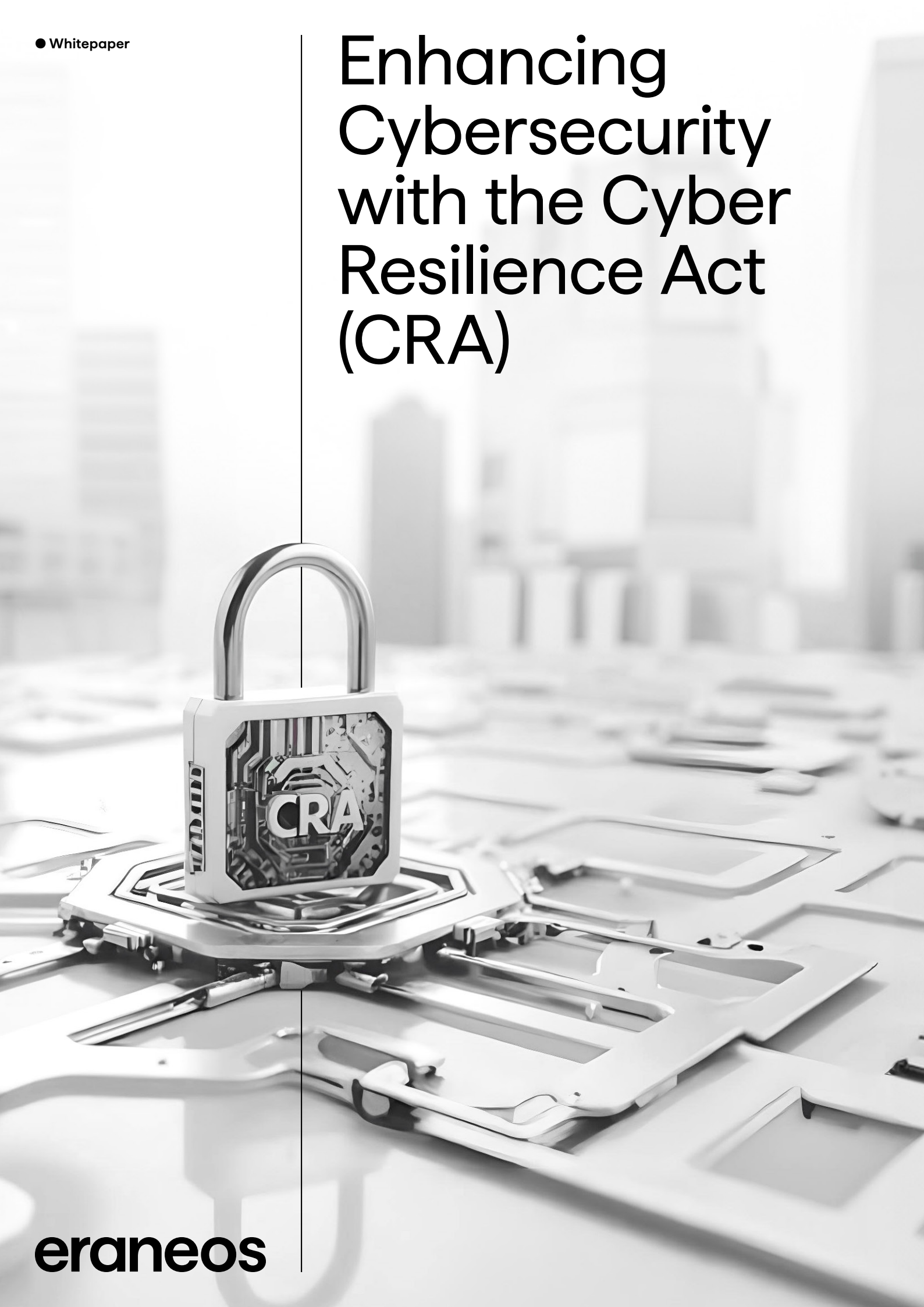
● Whitepaper

Enhancing Cybersecurity with the Cyber Resilience Act (CRA)



eraneos

Contents

Introduction 03

Background and context 04

Key provisions of the CRA 06

Impact on product security 07

Challenges and opportunities 08

AI-powered compliance: Navigating the cyber resilience act and beyond 09

Technical analysis & compliance strategies 12

Future directions 15

Conclusion 16

Appendices 17

Get in touch 19

Introduction

Cyber attacks can lead to significant financial losses, data breaches, and disruptions to critical infrastructure, highlighting the need for stringent cybersecurity measures.

Overview of the Cyber Resilience Act (CRA)

The CRA is a landmark regulation introduced by the European Union (EU) to enhance the cybersecurity of digital products available in the EU market. It aims to ensure that products with digital elements are designed, developed, and maintained with robust cybersecurity measures. The CRA addresses the increasing cybersecurity threats posed by the proliferation of digital devices and interconnected systems.

Importance of cybersecurity in the digital age

In today‘s interconnected world, cybersecurity is paramount. With the proliferation of digital devices and the increasing sophistication of cyber threats, ensuring the security of digital products is critical to protecting personal data, maintaining consumer trust, and safeguarding economic stability. Cyberattacks can lead to significant financial losses, data breaches, and disruptions to critical infrastructure, highlighting the need for stringent cybersecurity measures.

Objectives of the whitepaper

This whitepaper aims to provide a comprehensive overview of the CRA, its key provisions, and its impact on product security. It also explores the challenges and opportunities presented by the CRA, offering insights into best practices for compliance and future directions in cybersecurity legislation.

Background and context

By mandating robust cybersecurity measures, the CRA ensures that products with digital elements are designed, developed, and maintained with security as a priority.

Nabeel Siddiqie
Cybersecurity Partner - Eraneos

nabeel.siddiqie@eraneos.com

Historical context and development of the CRA

The CRA was developed in response to the growing need for a unified approach to cybersecurity across the EU. It builds on previous regulations, such as the NIS2 Directive and the Cybersecurity Act, to address gaps and enhance the overall security framework. It is therefore complementing the NIS2 Directive and further extends security requirements to product manufacturers. The CRA was proposed by the European Commission on September 15, 2022, and after extensive consultations and amendments, it was adopted by the European Parliament and the Council in October 2024, becoming effective in all EU countries on December 11, 2024 (unlike NIS2 which must be translated into national laws).

Comparison with previous cybersecurity regulations

Unlike previous regulations that focused primarily on critical infrastructure, the CRA extends its scope to include all products with digital elements. This comprehensive approach ensures that a wider range of devices and systems are covered, providing a more robust defense against cyber threats. The CRA also introduces new requirements for manufacturers, importers, and distributors, ensuring that cybersecurity is considered at every stage of the product‘s lifecycle.

Enhancing consumer trust

The CRA plays a pivotal role in enhancing consumer trust in digital products. By mandating robust cybersecurity measures, the CRA ensures that products with digital elements are designed, developed, and maintained with security as a priority. This proactive approach to cybersecurity helps protect personal data and reduces the risk of cyberattacks, thereby fostering greater confidence among consumers. As a result, when consumers trust that their data is secure, they are more likely to engage with digital products and services, which leads to increased adoption and satisfaction.

The CRA involves various stakeholders, including manufacturers, importers, distributors, and regulatory bodies.

Fostering innovation in the digital economy

The CRA not only addresses cybersecurity challenges but also fosters innovation in the digital economy. By setting high standards for cybersecurity, the CRA encourages manufacturers and vendors to develop innovative solutions that meet these requirements. This drive for innovation can lead to the creation of new technologies and products that are both secure and user-friendly. Additionally, the CRA's emphasis on regular security updates and vulnerability management ensures that digital products remain resilient against emerging threats, further promoting a culture of continuous improvement and innovation in the industry.

Key stakeholders and their roles

The CRA involves various stakeholders, including manufacturers, importers, distributors, and regulatory bodies. Each plays a crucial role in ensuring compliance and enhancing the cybersecurity landscape. Manufacturers are responsible for implementing cybersecurity measures during the design and development of products, while importers and distributors must ensure that products meet the CRA's requirements before they are placed on the market.

Key provisions of the CRA

- Mandatory cybersecurity requirements for digital products

The CRA sets out mandatory cybersecurity requirements for digital products, including secure-by-design principles, regular security updates, and vulnerability management. These requirements apply to both hardware and software components, ensuring that all aspects of a product are secure. Failure to comply may result in fines up to 15 million Euro or up to 2,5 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

- Obligations for manufacturers and vendors

Manufacturers and vendors are required to implement and maintain robust cybersecurity measures throughout the product lifecycle. This includes conducting risk assessments, providing security updates, and ensuring that products meet the CRA‘s standards before entering the market. Manufacturers must also provide clear and transparent information about the cybersecurity features of their products.

- Compliance timelines and enforcement mechanisms

The CRA outlines specific timelines for compliance and establishes enforcement mechanisms to ensure adherence. Non-compliance can result in significant penalties, emphasizing the importance of meeting the CRA‘s requirements. The main portion of the regulation will apply from December 2027, giving businesses time to adapt to the new requirements. Organizations must start reporting incidents and vulnerabilities to the designated bodies from September 2026.

Impact on product security

Michel Dieben
Senior Manager - Cybersecurity
Eraneos

michel.dieben@eraneos.com

Enhanced security measures for hardware and software

The CRA mandates enhanced security measures for both hardware and software components of digital products. This includes secure coding practices, regular security testing, and the implementation of security patches. By addressing vulnerabilities early in the development process, manufacturers can reduce the risk of cyberattacks and improve the overall security of their products.

Requirements for software updates and vulnerability management

Manufacturers must provide timely software updates to address vulnerabilities and ensure ongoing product security. This proactive approach helps mitigate risks and protect users from emerging threats. Regular updates and patches are essential to maintaining the security of digital products, as new vulnerabilities are discovered and exploited by cybercriminals.

Case studies of potential security improvements

Several case studies highlight the potential security improvements resulting from the CRA. For example, smart home devices with enhanced security features can better protect user data and prevent unauthorized access. In another case, industrial control systems with robust cybersecurity measures can prevent disruptions to critical infrastructure and ensure the safety of operations.

Challenges and opportunities

The CRA is expected to have significant economic and social impacts, including increased consumer trust, reduced cyber incidents, and a more secure digital ecosystem.

Implementation challenges for businesses

Implementing the CRA poses several challenges for businesses, including the need for significant investment in cybersecurity measures and the complexity of meeting regulatory requirements. Small and medium-sized enterprises (SMEs) may face difficulties in adapting to the new regulations due to limited resources and expertise. However, in the long term, it has the potential for return in investment by providing market access and competitive advantage, improving operational efficiency, strengthening customer trust and increasing investor and insurer confidence.

Opportunities for innovation in cybersecurity

Despite these challenges, the CRA also presents opportunities for innovation. Businesses can leverage the CRA to develop new cybersecurity solutions and enhance their competitive advantage. By investing in cybersecurity, organizations can differentiate themselves in the market and build trust with consumers.

Potential economic and social impacts

The CRA is expected to have significant economic and social impacts, including increased consumer trust, reduced cyber incidents, and a more secure digital ecosystem. Enhanced cybersecurity measures can lead to cost savings by preventing data breaches and reducing the need for costly incident response efforts.

AI-powered compliance: Navigating the cyber resilience act and beyond

Regulations like the CRA present significant compliance challenges for organizations, demanding substantial investment and expertise. Fortunately, Artificial Intelligence (AI) is rapidly becoming an indispensable ally, offering innovative solutions to streamline compliance, reduce manual workloads, and proactively manage the complexities of the CRA and similar cybersecurity regulations. This section explores how AI can act as a „compliance co-pilot," empowering organizations to efficiently meet the demands of the CRA and navigate the evolving regulatory landscape with greater agility and reduced risk.

Navigating regulatory complexity with AI: AI as your compliance co-pilot

Organizations today face a constantly shifting regulatory landscape, from privacy rules and sustainability mandates to industry-specific compliance frameworks.

AI has emerged as a valuable ally in this environment, capable of rapidly analyzing complex legal documents, identifying compliance gaps, and reducing manual workloads. By streamlining compliance efforts, AI empowers teams to focus on strategic, high-value tasks instead of getting stuck in repetitive checks and administrative duties. At Eraneos, we have seen first-hand how AI can unlock new efficiencies while maintaining strict standards in a variety of sectors.

Our experience shows that the most effective AI solutions integrate seamlessly with existing legal and operational processes, ensuring both agility and transparency. The following capabilities illustrate how organizations can harness AI to stay ahead of regulatory demands and reduce time-to-market risks, specifically in the context of regulations like the CRA. While AI offers powerful capabilities, successful CRA compliance is not solely about technology. Organizations need expert guidance to strategically implement AI tools, interpret AI-driven insights within their specific business context, develop comprehensive compliance strategies, and ensure ongoing adaptation to the evolving regulatory landscape. This is where expert consultancy and services become invaluable.

Key AI-driven capabilities for CRA compliance

01. Document & contract management - accelerating CRA readiness

AI-assisted CRA summaries:
AI can swiftly analyze the full text of the CRA and related guidance documents, helping to extract key obligations, timelines, and technical requirements. This provides compliance teams with rapid summaries, saving significant time in understanding the intricacies of the Act. Human experts are still needed to interpret these summaries in the context of the organization's specific products and business.

AI-enhanced CRA-aligned drafting & generation:
Leveraging AI, manufacturers can automate aspects of the drafting of compliance documentation, such as security policies, vulnerability disclosure procedures, and incident response plans, ensuring initial alignment with CRA requirements and reducing manual drafting efforts. However, human legal and compliance professionals must review and refine these drafts to ensure accuracy, completeness, and strategic alignment.

Real-time CRA updates:
AI tools can continuously monitor regulatory updates and amendments to the CRA, alerting organizations to necessary changes in their compliance strategies and preventing them from operating with outdated information. This monitoring provides valuable alerts, but human experts are required to assess the impact of these updates and adjust compliance strategies accordingly.

02. Compliance & risk analysis - proactive CRA management

AI-powered CRA gap identification:
By mapping CRA requirements against internal product development lifecycles, security measures, and documentation processes, AI can swiftly assist in pinpointing gaps in compliance. For example, AI can analyze if secure-by-design principles are adequately implemented in the design phase as mandated by the CRA. This gap identification is a starting point; human experts are needed to validate these gaps and develop remediation plans.

AI-driven CRA risk prioritization:
AI can help assess and prioritize cybersecurity risks associated with digital products based on CRA risk classifications and potential impact, enabling businesses to focus resources on the most critical areas for CRA compliance and mitigation. Risk prioritization requires human judgment to consider business context, risk appetite, and strategic priorities, going beyond AI-driven assessments.

AI-supported proactive CRA mitigation:
AI can analyze historical vulnerability data and industry best practices to suggest proactive measures for mitigating risks and ensuring continuous CRA compliance, such as recommending specific security testing methodologies or vulnerability management tools. These suggestions are valuable inputs, but human security experts must evaluate and tailor these recommendations to the organization's specific environment and resources.

03. Operational AI tools - streamlining CRA processes

CRA knowledgebases & chatbots:
AI-powered chatbots can be deployed internally to provide instant answers to employee queries regarding CRA requirements, internal policies, and compliance procedures, reducing the burden on specialist teams and ensuring consistent understanding across the organization. These chatbots provide initial support, but complex or nuanced questions will still require human expert intervention.

AI-assisted CRA supplier evaluation:
For manufacturers relying on third-party components, AI can assist in assessing supplier compliance with CRA requirements by analyzing certifications, security documentation, and audit reports, ensuring the entire product ecosystem aligns with the regulation.AI can flag potential issues, but human due diligence and expert review of supplier documentation remain crucial.

Building effective AI-driven CRA compliance solutions

While AI offers transformative potential for CRA compliance and risk management, successful implementation requires careful consideration beyond just the technology. These core considerations are crucial for ensuring AI-driven regulatory solutions are effective, transparent, and aligned with the evolving CRA landscape:

01.
Data quality & governance for CRA:

AI's effectiveness in CRA compliance hinges on high-quality data. Organizations must ensure that regulatory texts, product documentation, vulnerability data, and security logs are accurate, consistently updated, and properly governed to feed AI models effectively.

02.
Cross-functional collaboration for CRA:

CRA compliance necessitates collaboration across various departments, including product development, security, legal, and compliance. AI implementation should be a collaborative effort, ensuring insights are integrated across teams for holistic CRA adherence.

03.
Human oversight in CRA compliance:

While AI can automate many CRA compliance tasks, human expert oversight remains essential. AI should be viewed as a tool to augment human capabilities, with final decisions on CRA compliance strategies and risk assessments guided by human judgment and expertise.

04.
Ethical & privacy considerations for CRA:

AI systems used for CRA compliance must adhere to data protection regulations like GDPR, especially when processing personal data related to vulnerability reporting or user data security. Transparency in AI's data processing and interpretation builds trust and ensures ethical CRA compliance.

05.
Continuous improvement for evolving CRA:

The CRA and the broader cybersecurity landscape are dynamic. AI models for CRA compliance require continuous retraining and refinement to stay current with regulatory updates, emerging threats, and evolving best practices, ensuring long-term effectiveness.

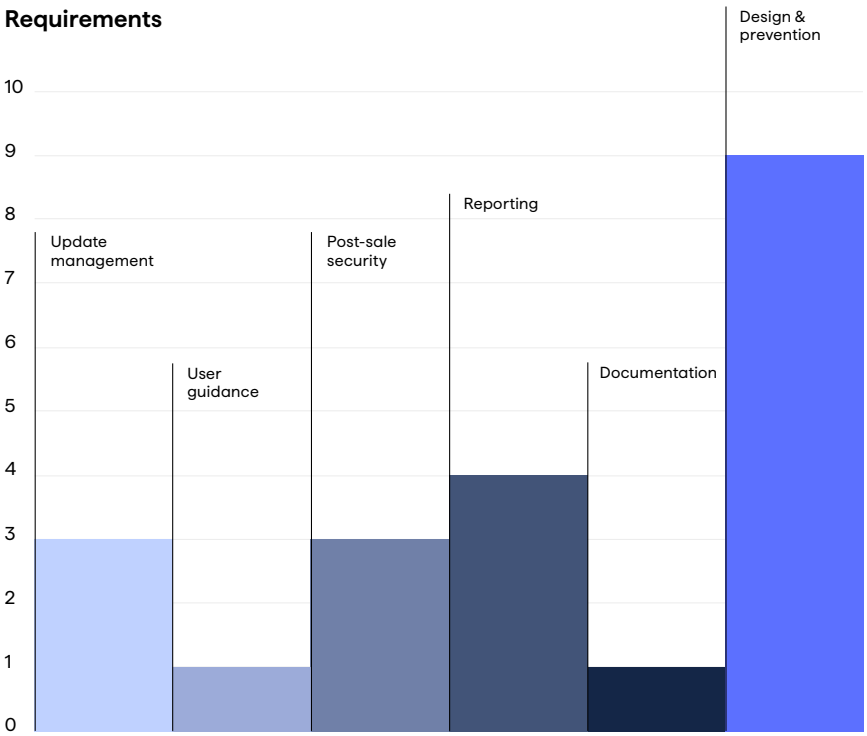
AI is revolutionizing how organizations approach regulatory compliance, offering tangible benefits for navigating the complexities of the CRA. By strategically implementing AI-powered tools and adhering to core principles of data governance, human oversight, and continuous improvement, businesses can achieve more efficient, proactive, and robust compliance with the CRA, ultimately enhancing the security of digital products and fostering greater consumer trust in the digital ecosystem.

Embracing AI for CRA compliance is a strategic imperative, but realizing its full potential requires expert guidance to navigate implementation, interpret results, and integrate AI into a broader, human-led compliance strategy. Organizations seeking to maximize the benefits of AI for CRA compliance and beyond should consider partnering with experienced cybersecurity and compliance professionals.

Technical analysis & compliance strategies

In-depth analysis of security requirements

The CRA's 21 security requirements can be categorized into six key areas. The chart below demonstrates the requirements heavily emphasize controls during the product's design phase, ensuring robust security measures are implemented from the outset.



Compliance strategies

To effectively comply with the CRA, consider the following strategies:

In **Design and prevention**, it is imperative for organizations to embed cybersecurity measures from the conceptual stages of product development, ensuring all products with digital elements are designed with a secure-by-default configuration. This involves rigorous risk assessments and ongoing vulnerability management, including securing against unauthorized access through advanced authentication and identity management systems. The integrity and confidentiality of data, whether stored, processed, or in transit, must be protected using cutting-edge encryption techniques and other relevant security methods. Moreover, the architecture of the product should be crafted to minimize attack surfaces and enhance resilience against potential disruptions, like denial-of-service attacks. AI-powered tools can assist in threat modeling during the design phase and automate security testing to ensure secure-by-design principles are effectively implemented for CRA compliance.

Documentation plays a critical role, requiring manufacturers to meticulously document all vulnerabilities and components, including a comprehensive software bill of materials in a commonly used and machine-readable format. This ensures traceability and accountability throughout the product's lifecycle and aids in regulatory compliance. It's essential for manufacturers to maintain these records for an extended period, facilitating ongoing oversight and adherence to cybersecurity regulations. AI can automate the generation and maintenance of software bill of materials (SBOMs) and other CRA-required documentation, significantly reducing manual effort and improving accuracy.

In the realm of **Reporting**, organizations must establish protocols for regular security testing and the transparent reporting of any vulnerabilities. This includes the public disclosure of vulnerabilities once they have been addressed, detailing the nature and severity of the vulnerabilities, and providing clear, accessible guidance for remediation. Furthermore, a policy for coordinated vulnerability disclosure should be enforced to streamline communication between the manufacturer and the cybersecurity community, enhancing the overall security ecosystem. AI can automate security testing processes, vulnerability scanning, and the generation of reports required for CRA compliance, enabling faster and more efficient reporting.

Post-sale security requires that products enter the market devoid of known exploitable vulnerabilities and that manufacturers remain vigilant, addressing new security threats swiftly. The strategy should include the separation of security updates from functionality updates to prevent the introduction of new vulnerabilities during routine updates. AI-driven vulnerability monitoring and threat intelligence platforms can proactively identify emerging threats and vulnerabilities, enabling faster post-sale security responses and ensuring continuous CRA compliance.

These comprehensive strategies allow companies to ensure robust cybersecurity compliance, safeguard user data, and maintain the integrity and reliability of their products in a rapidly evolving digital landscape.

User guidance should focus on enabling users to manage their data securely and intuitively, providing tools for the easy removal and secure transfer of personal settings and data. Instructions for these processes should be straightforward and integrated into the product design, ensuring they are accessible and understandable throughout the product's usable life. AI-powered chatbots and virtual assistants can enhance user guidance by providing instant support and clear instructions on security best practices and data management, improving user understanding of CRA-related security features.

Lastly, **Update management** must ensure that products can receive security updates in a timely and secure manner. This includes setting updates to install automatically by default, while also offering users the flexibility to opt out or delay these updates if necessary. Organizations must also provide clear and timely advisory messages about updates to help users understand and perform essential security actions without undue delay. AI can automate the deployment and tracking of security updates, ensuring timely patching of vulnerabilities and efficient update management as required by the CRA.

By following these comprehensive strategies, and strategically leveraging AI-powered tools across various compliance domains, organizations can not only ensure robust cybersecurity compliance, safeguard user data, and maintain the integrity and reliability of their products in a rapidly evolving digital landscape, but also efficiently and effectively meet the specific requirements of the CRA.

Future directions

Anticipated developments in cybersecurity legislation

The cybersecurity landscape is constantly evolving, and new legislation is expected to emerge in response to emerging threats and evolving security needs. For instance, the NIS2 Directive, which strengthens cybersecurity resilience and harmonizes regulations across the EU, came into effect in August 2024. Similarly, the United States has introduced new cybersecurity rules, including the SEC‘s Cyber Disclosure Rule, which requires organizations to report material cybersecurity incidents within four business days.

These developments indicate a trend towards more stringent and comprehensive cybersecurity regulations globally. The integration of AI in compliance strategies will likely become even more critical as regulations become more complex and data-driven, and as organizations seek more efficient and scalable ways to manage their growing compliance obligations.

Conclusion

The CRA is expected to have a profound impact on the cybersecurity landscape, driving improvements in product security and fostering a more secure digital ecosystem.

Final thoughts

The CRA represents a significant step forward in enhancing cybersecurity across the EU. By setting high standards for digital products, the CRA helps protect consumers and businesses from cyber threats. The regulation mandates secure-by-design principles, regular security updates, and robust incident reporting mechanisms, ensuring that products with digital elements are secure throughout their lifecycle.

CRA‘s impact on cybersecurity

The CRA is expected to have a profound impact on the cybersecurity landscape, driving improvements in product security and fostering a more secure digital ecosystem. By addressing vulnerabilities early in the development process and ensuring ongoing security maintenance, the CRA helps mitigate risks and build consumer trust in digital products. Furthermore, embracing innovative solutions like AI-powered compliance tools will be crucial for organizations to effectively navigate and thrive in this evolving regulatory environment, turning compliance challenges into opportunities for innovation and competitive advantage.

Call to action for stakeholders

All stakeholders, including businesses, regulatory bodies, and consumers, must work together to ensure the successful implementation of the CRA and enhance cybersecurity across the EU. Businesses should invest in cybersecurity measures and comply with the CRA‘s requirements and strategically explore and leverage AI to streamline these efforts, realizing significant gains in efficiency, accuracy, and proactive risk management, while regulatory bodies should provide guidance and support to facilitate this transition. Consumers should stay informed about cybersecurity risks and take proactive steps to protect their digital assets, benefiting from the enhanced security and transparency fostered by the CRA and enabled by AI-driven compliance solutions.

Appendices

Categorization of the rules as written in the EU Cyber Resilience Act (EU 2024/2847)

01. Design and prevention

- Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state. (Annex 1, Part 1, Article 2 b)

- Products with digital elements shall ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorized access. (Annex 1, Part 1, Article 2 d)

- Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means. (Annex 1, Part 1, Article 2 e)

- Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, and report on corruptions. (Annex 1, Part 1, Article 2 f)

- Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation). (Annex 1, Part 1, Article 2 g)

- Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks. (Annex 1, Part 1, Article 2 h)

- Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces. (Annex 1, Part 1, Article 2 j)

- Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques. (Annex 1, Part 1, Article 2 k)

- Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user. (Annex 1, Part 1, Article 2 l)

02. Documentation

- Manufacturers of products with digital elements shall identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products. (Annex 1, Part 2, Article 1)

03. Reporting

- Manufacturers of products with digital elements shall apply effective and regular tests and reviews of the security of the product with digital elements. (Annex 1, Part 2, Article 3)

- Manufacturers of products with digital elements shall once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch. (Annex 1, Part 2, Article 4)

- Manufacturers of products with digital elements shall put in place and enforce a policy on coordinated vulnerability disclosure. (Annex 1, Part 2, Article 5)

- Manufacturers of products with digital elements shall take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements. (Annex 1, Part 2, Article 6)

04. Post-sale security

- Products with digital elements shall be made available on the market without known exploitable vulnerabilities. (Annex 1, Part 1, Article 2 a)

- Manufacturers of products with digital elements shall minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks. (Annex 1, Part 1, Article 2 i)

- Manufacturers of products with digital elements shall in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates. (Annex 1, Part 2, Article 6)

05. User guidance

- Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner. (Annex 1, Part 1, Article 2 m)

6. Update management

- Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them. (Annex 1, Part 1, Article 2 c)

- Manufacturers of products with digital elements shall provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner. (Annex 1, Part 2, Article 7)

- Manufacturers of products with digital elements shall ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. (Annex 1, Part 2, Article 8)

Additional resources

- European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/

- NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

- Cyber Resilience Act: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

- SEC Cyber Disclosure Rule: https://www.sec.gov/rules/final/2022/33-11038.pdf

Get in touch

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

Michel Dieben
Senior Manager - Cybersecurity
Eraneos
michel.dieben@eraneos.com

Eraneos Netherlands
De Passage 126-136
1101 AX Amsterdam
+31 20 305 3700
info.nl@eraneos.com
eraneos.nl