AI & Partners

Amsterdam - London - Singapore

EU AI Act

Cyber Resilience Act versus EU AI Act

A Mapping Exercise

September 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Dr. Amritha Subhayan Krishnan, Smart Story Labs

Arnoud Engelfriet, ICTRecht

Indra Joshi, OptumUK

Maryam Ghadrdan (PhD), Planck Technologies

Debbie Reynolds, Global Data Advisor

Principles

EU AI Act Vs CRA

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

AI & Partners

Amsterdam - London - Singapore

Who Are We

AI That You Can Trust

Why Us?

Stay on the right side of history. At AI & Partners, we believe AI should unlock potential—not cause harm. We've seen the fear and fallout when teams lose control of AI, but also the trust and innovation that follow when it's handled responsibly. That's why we exist: to help you build AI you can trust and stand behind—for the long run.

80%

of AI systems are unknown

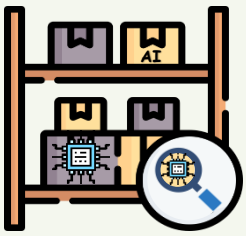
What Do We Do?

We enable safe AI usage—for your organization and your clients. Unknown AI adoption leads to confusion, risk, and reputational damage. We help you take control with tools to identify, monitor, and govern all AI systems—so you're not reacting to AI, you're leading it.

How Do We Do It?

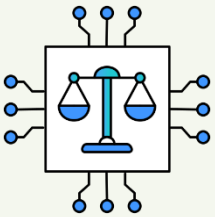
Do you know what AI systems you have? Identify all known and unknown AI systems (algorithms, LLMs, prompts, and models) from all internal and external AI vendors, automated by generating your inventory. Overall, 80% of AI inventory is unknown to our clients.

How do you guarantee ongoing safe AI use? Continuously monitor deployed AI systems for performance drift, anomalies or failures, real-world impacts, and emerging risks (e.g. data poisoning). Any malfunction of an AI system has severe implications for organisations (e.g. inability to assess online misinformation that leads to widespread public mistrust), so monitoring becomes a matter of urgency.



AI Discovery & AI Inventory

Automatically detect all AI systems, including models, algorithms, and prompts, and maintain a live, always-updated register for full visibility and compliance.



Responsible AI

Embed fairness, transparency, and control into every stage of AI use—aligning with the EU AI Act and building 'Trustworthy-by-Design'.

Model Monitoring

Continuously track your AI models after deployment to detect drift, bias, or failure—so you stay in control and prevent harm before it happens.

Contents

Introduction

As artificial intelligence reshapes global economic and governance landscapes, regulatory approaches are rapidly emerging to guide its responsible development and deployment. The European Union's Artificial Intelligence Act (AI Act) sets a legally binding framework for high-risk AI systems, grounded in principles of human oversight, transparency, and risk management. Alongside it, the EU's Cyber Resilience Act (CRA) introduces mandatory cybersecurity standards for all digital products—hardware and software—ensuring a lifecycle approach to digital safety, secure design, and resilience.

This report presents a comparative mapping of the EU AI Act against the Cyber Resilience Act, designed to help stakeholders understand how these interrelated regulatory frameworks align and diverge. It identifies key thematic intersections—such as secure-by-design principles, market surveillance, CE marking, conformity assessment, vulnerability disclosure, and public-private coordination—that define the EU's evolving approach to AI and cybersecurity co-regulation.

As a result of exploring these cross-legislative connections, the report supports legal advisors, cybersecurity architects, AI developers, and compliance leaders in interpreting how cybersecurity regulation (CRA) can reinforce AI-specific governance (AI Act), and vice versa. It encourages organizations to view the CRA not merely as a digital product regulation, but as an integral part of the trustworthy AI ecosystem the EU is cultivating through comprehensive policy convergence.

Whether you are designing AI-enabled products, updating cybersecurity protocols, or managing regulatory risks, this report provides actionable insights for integrating the CRA's cybersecurity requirements with AI Act obligations—building AI that is both functionally secure and legally compliant across Europe's digital single market. By aligning lifecycle cybersecurity with AI-specific risk governance, organizations can meet current standards while preparing for the next wave of integrated, interoperable regulation.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about Cyber Resilience Act

1. What is the Cyber Resilience Act (CRA)?

The Cyber Resilience Act is a new EU regulation introducing mandatory cybersecurity standards for products with digital elements—both hardware and software—sold within the EU. It aims to ensure better protection against cyber threats by requiring manufacturers to embed security features throughout a product's lifecycle. The CRA mandates updates, secure design, and transparency, enhancing trust and safety for consumers and businesses alike. It complements existing legislation like the NIS2 Directive, creating a harmonized regulatory framework to reduce cybersecurity risks and increase resilience across the internal market.

2. Why is the CRA necessary?

Cybersecurity threats are increasingly targeting everyday digital products. Many devices lack adequate protection, and manufacturers often neglect to provide timely security updates. This leaves consumers vulnerable and shifts the burden of risk away from producers. The CRA addresses these issues by enforcing design-phase security requirements and obligating support for updates during a product's expected lifecycle. It ensures consumers and businesses get accurate cybersecurity information and helps reduce the spread of cyber threats across the EU, fostering a safer and more secure digital environment for all stakeholders.

3. Which products are affected by the CRA?

The CRA applies to all "products with digital elements" that are connected—wired or wirelessly—to the internet and are marketed in the EU. This includes smart home devices, connected toys, wearable tech, industrial software, and more. Whether it's hardware or embedded software, if it's sold as a standalone product and has digital capabilities, it must meet the CRA's essential cybersecurity requirements. However, software offered exclusively as a service (e.g., SaaS platforms) is not covered, although other laws like the NIS2 Directive may still apply.

4. What cybersecurity requirements must manufacturers meet?

Manufacturers must design products with cybersecurity in mind from the outset. They must conduct risk assessments, embed security features, and ensure safe default configurations. Products must be accompanied by clear, up-to-date instructions on security settings and maintenance. Manufacturers must define and honor a support period during which they provide security updates and vulnerability patches. Additionally, they must report exploited vulnerabilities and incidents to relevant authorities. The aim is to ensure that products remain secure throughout their lifecycle and that users are well-informed about cyber risks.

5. Who enforces the CRA, and how?

Each EU Member State will appoint a market surveillance authority to enforce the CRA. These authorities will have the power to investigate non-compliant products, require fixes, prohibit sales, and issue recalls. If manufacturers or other economic operators fail to comply, authorities can impose administrative fines—national laws will define these penalties within maximum levels set by the CRA. The system ensures products on the market meet uniform cybersecurity standards and gives regulators tools to swiftly respond to threats and protect both consumers and digital infrastructure.

6. How does the CRA affect consumers?

Consumers will benefit from improved digital product security and more transparent cybersecurity information. They'll have access to clear guidance on safe product use and receive security updates throughout a product's support period. This reduces the risk of data breaches, identity theft, and other cyber threats. Enhanced product labeling (via the CE mark) signals compliance with EU cybersecurity standards. The CRA also fosters greater trust in connected devices, helping consumers make informed purchasing decisions while ensuring their rights to data and privacy are better protected.

7. What does the CE marking mean under the CRA?

The CE marking under the CRA signifies that a product complies with the EU's cybersecurity requirements. Before placing a product on the market, manufacturers must conduct a conformity assessment to verify it meets all applicable CRA standards. Depending on the risk level of the product, this may involve self-assessment or third-party evaluation. Once conformity is confirmed, the CE mark can be affixed, enabling free movement of the product within the EU's single market. The mark assures consumers and businesses that the product is secure by design.

8. Are software services covered by the CRA?

No, the CRA specifically applies to products with digital elements that are sold as goods in the EU, not to software provided purely as a service (e.g., cloud-hosted platforms). However, cybersecurity for software services is addressed under other EU regulations, such as the NIS2 Directive. For instance, cloud service providers and electronic health systems are required to meet strict cybersecurity standards, even if they are not covered by the CRA. Together, these laws aim to create a comprehensive cybersecurity framework for both products and services.

9. What happens to non-compliant products under the CRA?

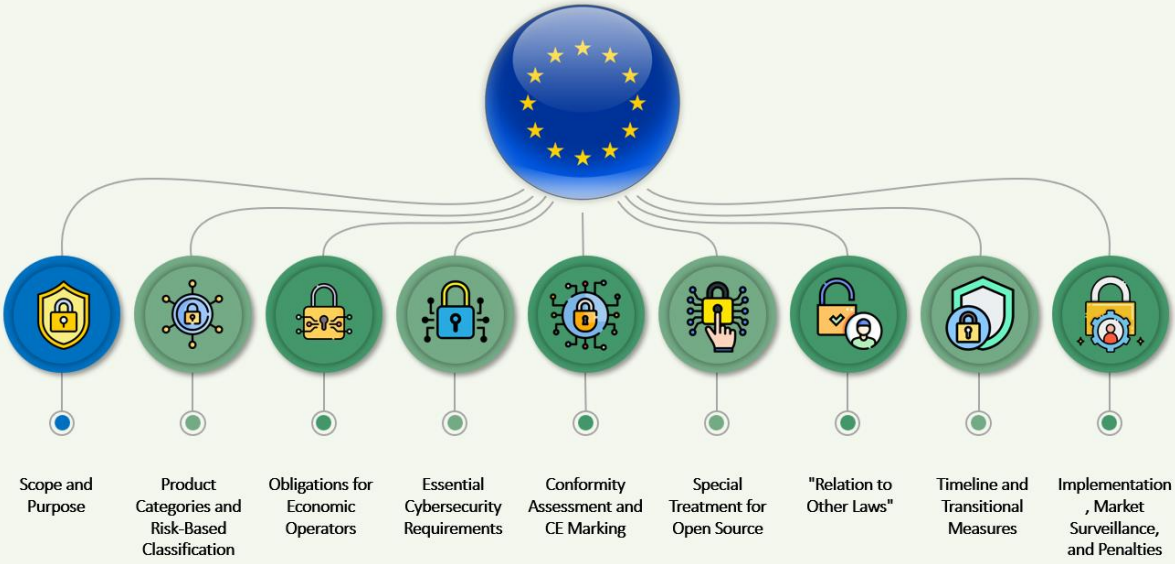
If a product fails to meet CRA requirements, market surveillance authorities can demand corrective action from the responsible parties. This may involve withdrawing the product from the market, halting sales, or recalling units already sold. Fines may be imposed on non-compliant companies, with amounts determined by national laws under the CRA's framework. These enforcement measures ensure that only products meeting robust cybersecurity standards are allowed to circulate within the EU, minimizing the risk posed by insecure digital technologies to individuals and businesses.

10. When will the CRA be enforced?

Following its adoption in 2024, the CRA includes a 36-month transition period for manufacturers and EU Member States to fully comply. However, certain obligations—like reporting actively exploited vulnerabilities—will come into effect sooner, just 21 months after the regulation enters into force. To support implementation, the European Commission will request the creation of harmonized standards by EU Standardisation Organisations. These technical specifications will guide manufacturers in aligning their products with CRA requirements and ensure a consistent, high level of cybersecurity across all digital products in the EU.

Understanding Cyber Resilience Act

Scope and Purpose



What are the key goals?

The Cyber Resilience Act (CRA) aims to ensure that all products with digital elements—hardware or software—are secure throughout their entire lifecycle. This includes both locally installed and remotely connected components, such as cloud services essential to a product's function. The main goal is to reduce vulnerabilities through secure design, risk assessment, and consistent support.

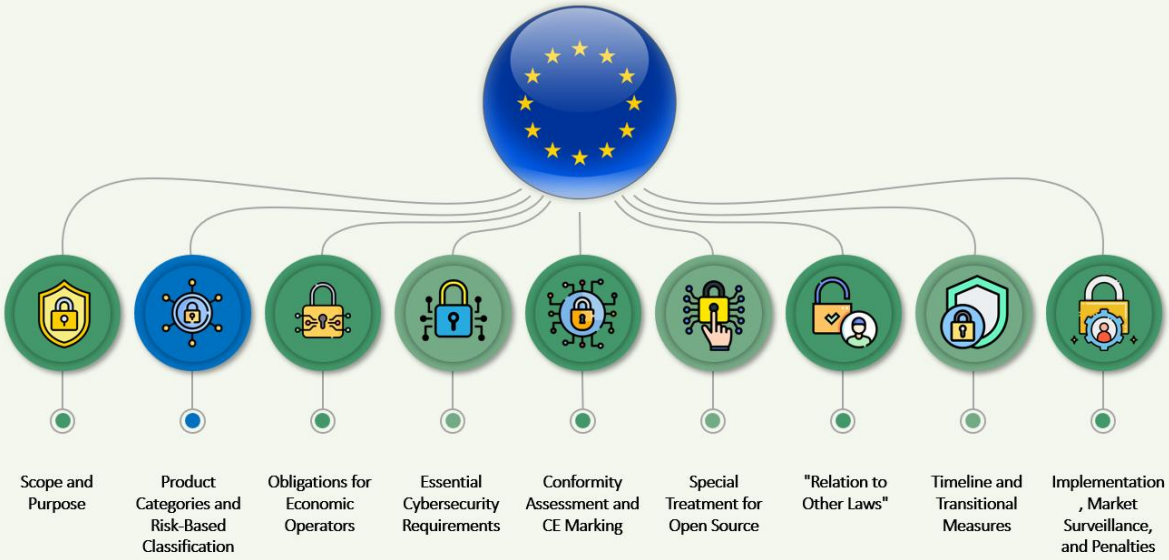
Why is it needed?

As digital products become more interconnected and complex, security gaps are increasingly exploited by malicious actors. Many manufacturers prioritize speed-to-market and features over robust security, leaving consumers and businesses vulnerable. Existing rules do not fully cover the entire product lifecycle or the ecosystem of remote services tied to these products. The CRA fills this gap by providing a comprehensive, EU-wide framework that addresses both on-device and cloud-based security risks.

How does it work in practice?

Manufacturers of digital products, including those using essential cloud components, must incorporate secure design principles and maintain cybersecurity throughout a product's lifecycle. This includes updating both firmware and supporting remote services. Products must meet essential cybersecurity requirements before entering the EU market. Compliance involves both internal security risk assessments and transparent communication with users.

Product Categories and Risk-Based Classification



What are the key goals?

The CRA establishes a tiered risk-based approach to regulate products with digital elements. Its goal is to tailor compliance obligations to the potential impact a product may have on cybersecurity. Products are divided into general, important (Class I), and critical (Class II) categories. Higher-risk products—like networking devices, identity systems, or industrial control software—face more stringent requirements and oversight. This classification system ensures proportionate regulation.

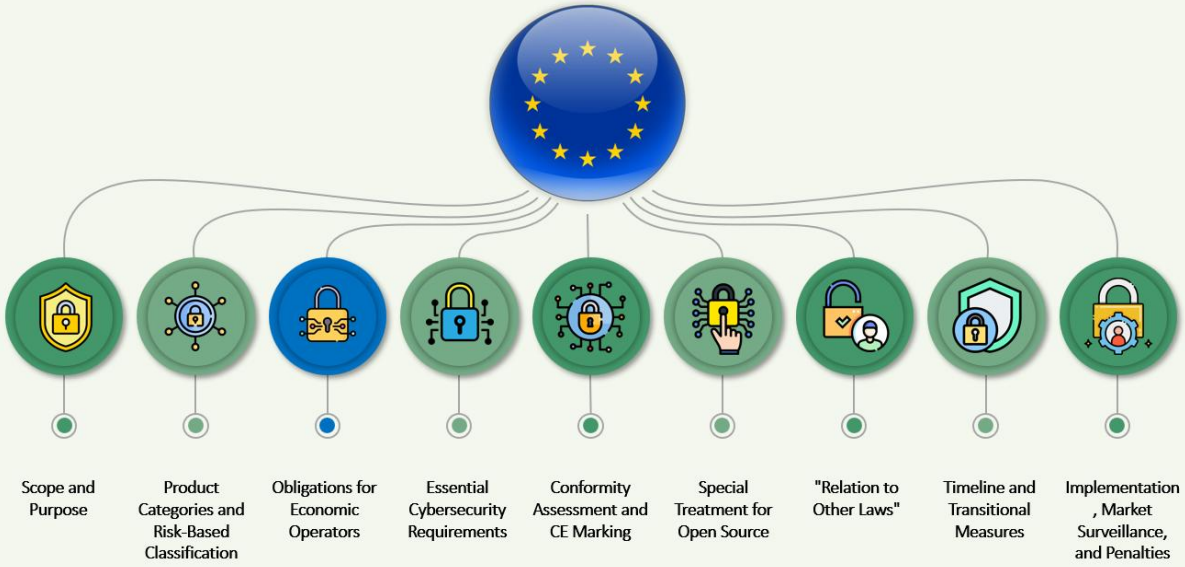
Why is it needed?

Not all digital products pose the same level of cybersecurity risk. A smartwatch differs significantly from industrial control software or secure authentication systems. A one-size-fits-all approach could either stifle innovation or leave high-risk systems under-protected. The CRA addresses this by classifying products based on impact potential. This allows regulators to focus on higher-risk items while offering more flexibility for low-risk products.

How does it work in practice?

Manufacturers must determine which risk class their product falls into based on defined criteria. General products undergo a self-assessment for compliance, while Class I (important) and Class II (critical) products must undergo third-party conformity assessments. The classification impacts everything from documentation and testing to who must review and validate the cybersecurity measures. Products like VPNs, firewalls, or authentication tools are examples of higher-risk categories.

Obligations for Economic Operators



What are the key goals?

Manufacturers must determine which risk class their product falls into based on defined criteria. General products undergo a self-assessment for compliance, while Class I (important) and Class II (critical) products must undergo third-party conformity assessments. The classification impacts everything from documentation and testing to who must review and validate the cybersecurity measures. Products like VPNs, firewalls, or authentication tools are examples of higher-risk categories.

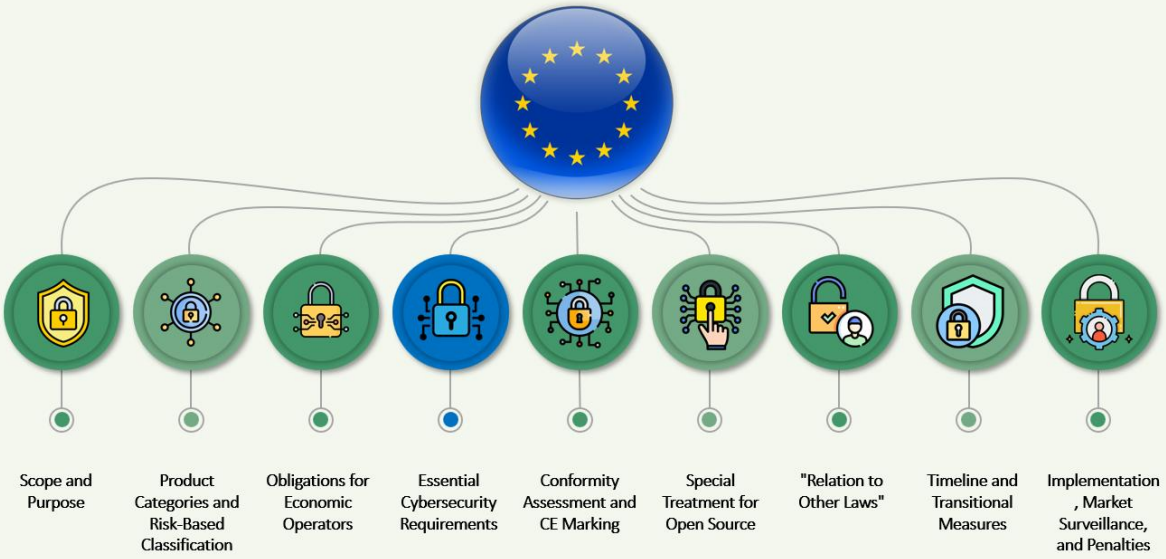
Why is it needed?

Many security lapses originate from unclear responsibilities or inconsistent practices across the supply chain. Without defined obligations, updates are neglected, flaws go unpatched, and insecure products remain in circulation. Consumers and businesses bear the consequences of these failures. By outlining duties for each role in the supply chain, the CRA ensures accountability. Everyone involved must take cybersecurity seriously, from initial design to post-sale support.

How does it work in practice?

Manufacturers must assess product risks, integrate security from the development phase, and deliver updates during the product's supported lifecycle. They must also provide documentation and transparency about risks and support periods. Importers check that products comply before selling them in the EU. Distributors must ensure products bear the CE mark and come with proper instructions. Authorities may audit or inspect any actor in the chain.

Essential Cybersecurity Requirements



What are the key goals?

The CRA establishes a list of essential cybersecurity requirements aimed at ensuring secure design, development, and maintenance of digital products. These include secure-by-default configurations, timely vulnerability patching, incident and vulnerability reporting, and transparency about security updates and support periods. The goal is to create a baseline of protection across all digital devices and software sold in the EU, ensuring users are protected from cyber threats but also kept informed about security measures of devices.

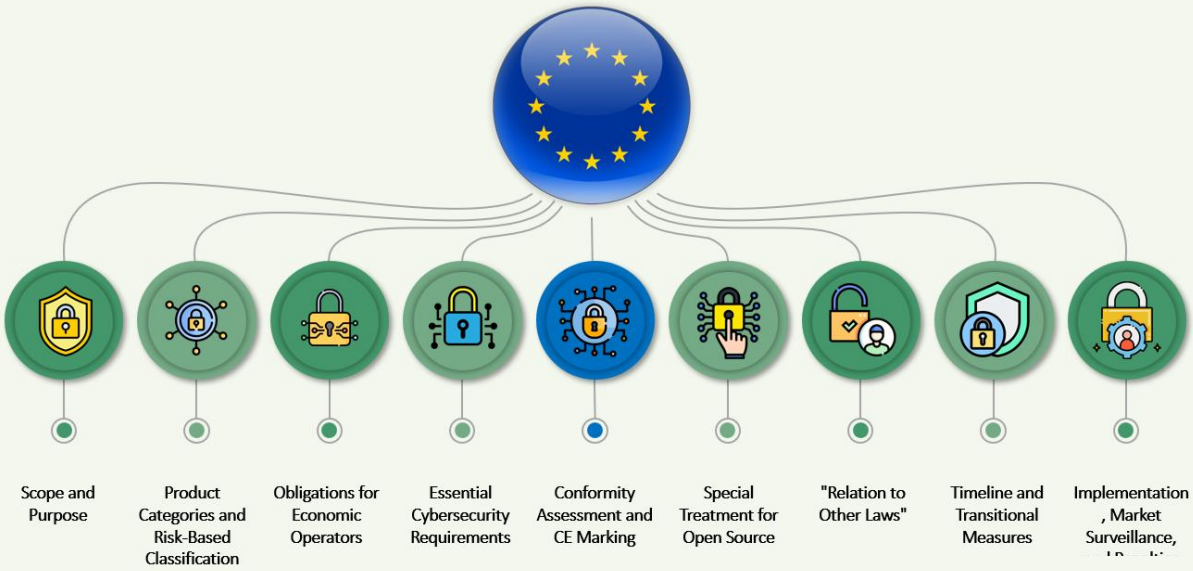
Why is it needed?

Many digital products are sold with insecure settings, unpatched vulnerabilities, or no plan for long-term support. This puts users at risk and allows attackers to exploit flaws for months or years. The CRA addresses this by making cybersecurity a required feature, not an afterthought. Consumers deserve products that are secure by design and keep them informed about updates and known issues.

How does it work in practice?

To comply with CRA cybersecurity requirements, manufacturers must follow secure development practices, minimize attack surfaces, and release patches for known issues during a defined support period. Security updates should be automatic by default but allow opt-out. Vulnerability disclosure must be coordinated and timely. Product documentation must clearly state the support timeline and potential cyber risks. Products failing to meet these standards cannot be sold in the EU.

Conformity Assessment and CE Marking



What are the key goals?

The CRA's goal here is to ensure that only products meeting essential cybersecurity requirements can be sold in the EU. This is achieved through conformity assessments and CE marking. The CE mark becomes the visual guarantee that a product has met the CRA's security standards. Products are evaluated either through internal assessments or third-party certification, depending on their risk classification. The ultimate aim is to harmonize cybersecurity across the EU, and provide assurance to users.

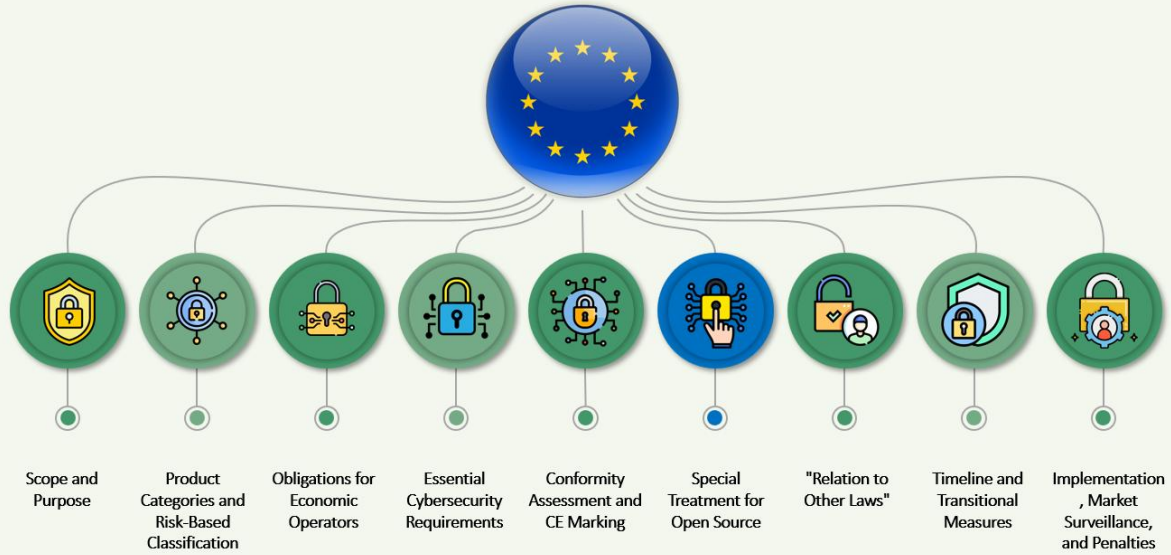
Why is it needed?

Without standard procedures for evaluating cybersecurity compliance, products of varying quality flood the market, exposing users to preventable threats. Inconsistent national rules also create confusion and fragmentation for businesses. The CRA resolves this by standardizing the assessment and approval process across the EU. By requiring that digital products demonstrate conformity before bearing the CE mark, the regulation increases accountability, and boosts trust among consumers and enterprise users alike.

How does it work in practice?

Manufacturers must carry out a risk-based assessment of their product's cybersecurity. Low-risk products may undergo internal evaluation, while higher-risk (Class I or II) products require third-party audits or certification. Once compliance is confirmed, the manufacturer issues an EU Declaration of Conformity and applies the CE mark to the product. This mark signifies that the product meets all applicable cybersecurity requirements under the CRA. Authorities may conduct spot-checks or require documentation.

Special Treatment for Open Source



What are the key goals?

The CRA seeks to balance innovation with accountability by treating open-source software (OSS) differently based on its use. Non-commercial OSS is exempt from full CRA obligations, recognizing its community-driven, volunteer-based development model. However, when open-source software is used commercially or provided as part of a product, compliance is required. The goal is to maintain a thriving open-source ecosystem while ensuring that widely-used OSS components, especially in commercial products.

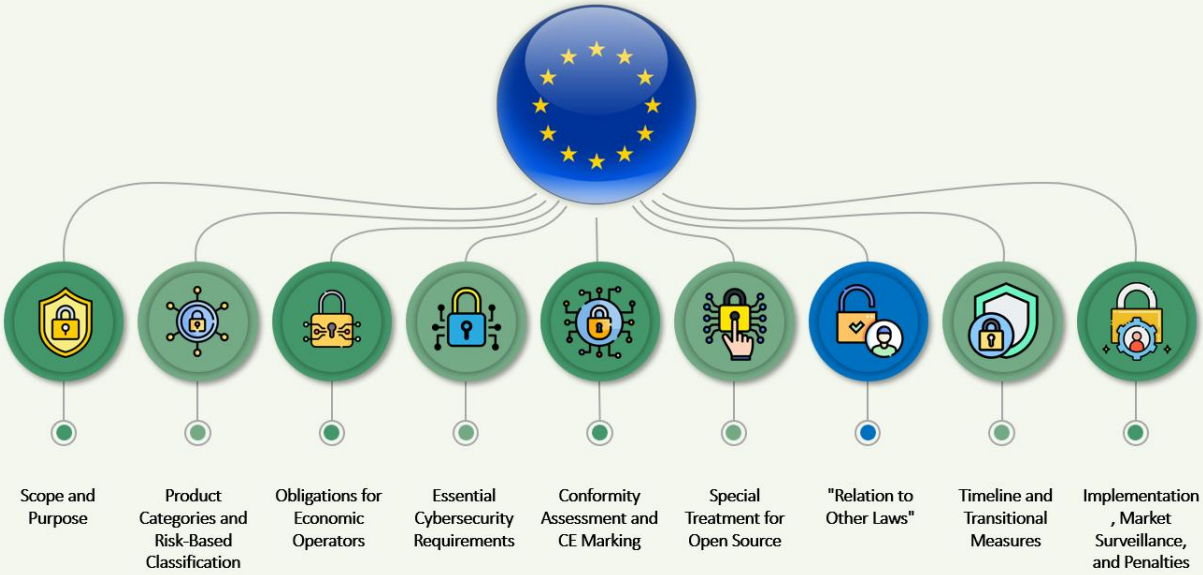
Why is it needed?

Open-source software is critical to modern digital infrastructure but often lacks formal support and structured security processes. Some widely used OSS libraries and tools are integrated into commercial products without proper vetting, creating hidden vulnerabilities. Blanket regulation would hinder open-source innovation. The CRA takes a nuanced approach: it exempts non-commercial projects but applies requirements when OSS is used in business or integrated into products.

How does it work in practice?

Individual developers or hobbyist OSS projects are not subject to the CRA. However, when open-source components are integrated into commercial products or provided as managed services, those responsible must ensure compliance. Foundations or stewards overseeing long-term OSS projects with infrastructure or financial support may also be subject to light regulatory obligations. This includes disclosing security vulnerabilities and maintaining update mechanisms.

Relation to Other Laws



What are the key goals?

The CRA is designed to complement, not conflict with, existing EU regulations such as the NIS2 Directive, GDPR, and the AI Act. Its goal is to fill a specific regulatory gap by targeting product-level cybersecurity, while existing frameworks often focus on organizational, data protection, or sector-specific requirements. The CRA aligns with these laws to create a comprehensive and harmonized cybersecurity landscape in the EU. It also ensures consistency in how products and services are secured, reported, and monitored.

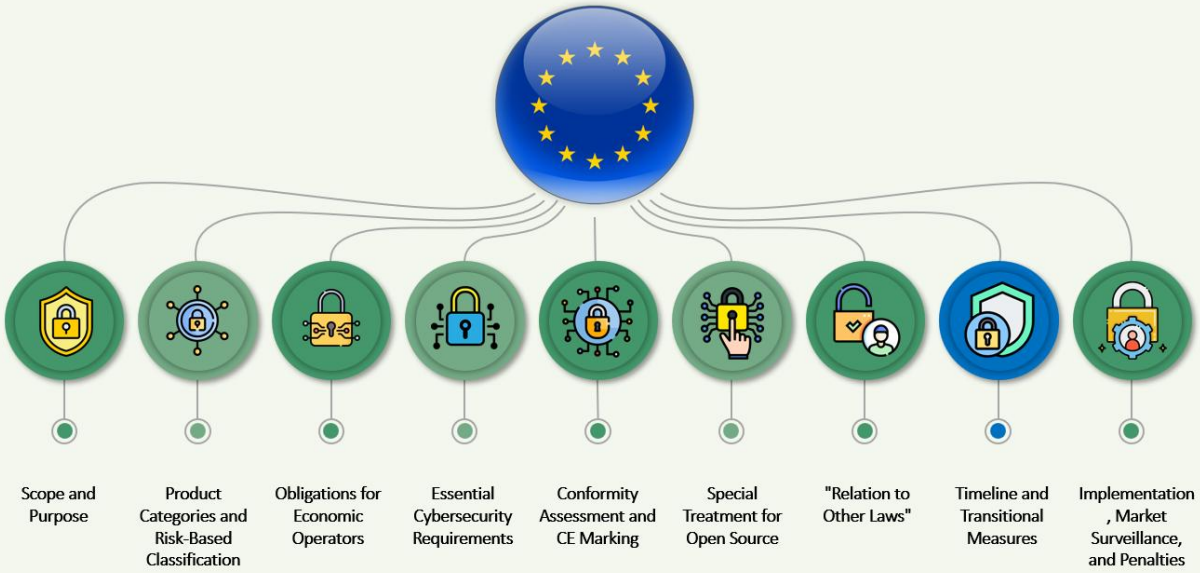
Why is it needed?

Cybersecurity laws in the EU have traditionally focused on critical infrastructure or data protection, leaving gaps in product security regulation. As threats increasingly arise from insecure digital devices, the CRA steps in to regulate the security of the products themselves. Coordination with existing laws ensures consistency and legal certainty for manufacturers and operators. To facilitate integration into the EU's broader legal framework, the CRA avoids duplication and enhances synergies, allowing businesses to build secure products and services without navigating overlapping obligations.

How does it work in practice?

The CRA builds on the New Legislative Framework and complements the NIS2 Directive's focus on critical services. For example, the CRA improves supply chain security by regulating the products used in NIS2-covered sectors. It aligns with GDPR by protecting devices handling personal data and with the AI Act by ensuring AI-enabled products are secure by design. If sector-specific rules already provide equal or stronger security standards, they may override CRA provisions.

Timeline and Transitional Measures



What are the key goals?

The CRA provides a structured timeline for compliance to avoid market disruption. The key goal is to give manufacturers, especially SMEs, enough time to adapt to the new requirements without halting innovation or product development. By phasing in the regulation, the EU ensures a smooth transition while maintaining its commitment to strengthening cybersecurity across the board.

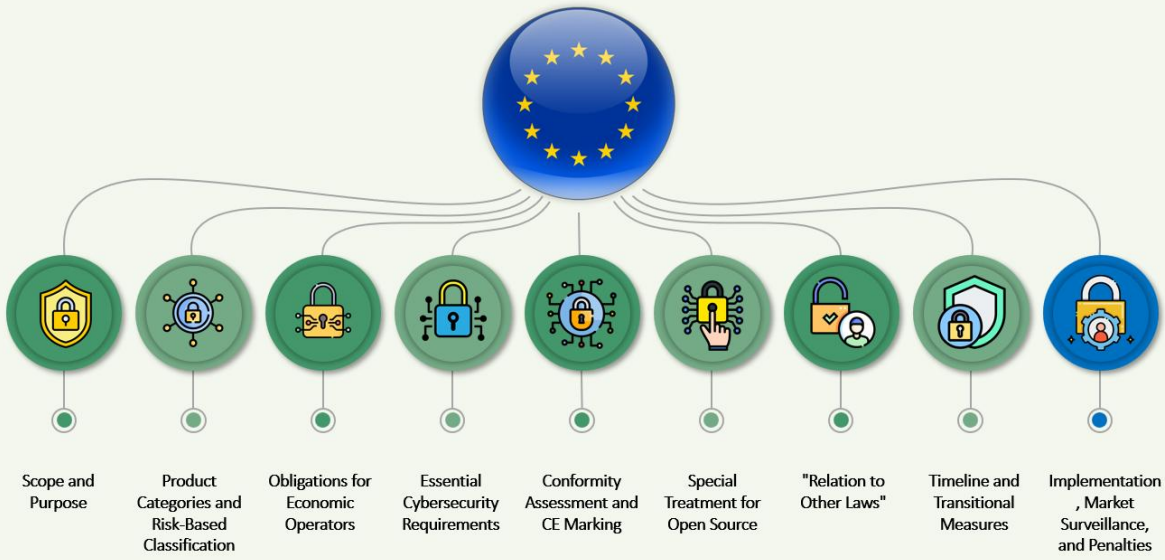
Why is it needed?

Immediate enforcement of new, complex cybersecurity requirements could overwhelm manufacturers and stall product development pipelines. It could also lead to supply chain delays or the withdrawal of non-compliant yet widely used products. The transitional approach allows time to prepare processes, documentation, and compliance systems. This is especially critical for small and medium-sized enterprises. It also enables regulators and standardization bodies to finalize technical specifications and offer clearer guidance.

How does it work in practice?

The CRA entered into force in November 2024, allowing economic operators until 11 December 2027 to comply with most provisions. However, reporting obligations for exploited vulnerabilities and incidents apply earlier—11 September 2026 —due to their critical importance. Products already on the market before the CRA's effective date are exempt unless significantly modified. During the transition, the European Commission will work with standards organizations to develop harmonized technical requirements.

Implementation, Market Surveillance, and Penalties



What are the key goals?

The CRA aims to enforce cybersecurity compliance consistently across the EU by empowering national market surveillance authorities. These authorities will oversee inspections, ensure non-compliant products are corrected or removed, and impose penalties where necessary. The goal is to create a proactive enforcement ecosystem that detects issues early, ensures security standards are followed, and holds all economic operators accountable. This also improves the EU's overall cybersecurity awareness and resilience.

Why is it needed?

Regulations without enforcement mechanisms are ineffective. To ensure that digital products meet the CRA's strict requirements, robust surveillance and enforcement are essential. Many manufacturers may be unaware of or resistant to these obligations without credible oversight. The CRA resolves this by mandating national authorities to monitor, audit, and penalize non-compliant actors. Additionally, coordinated surveillance helps identify systemic issues and recurring vulnerabilities.

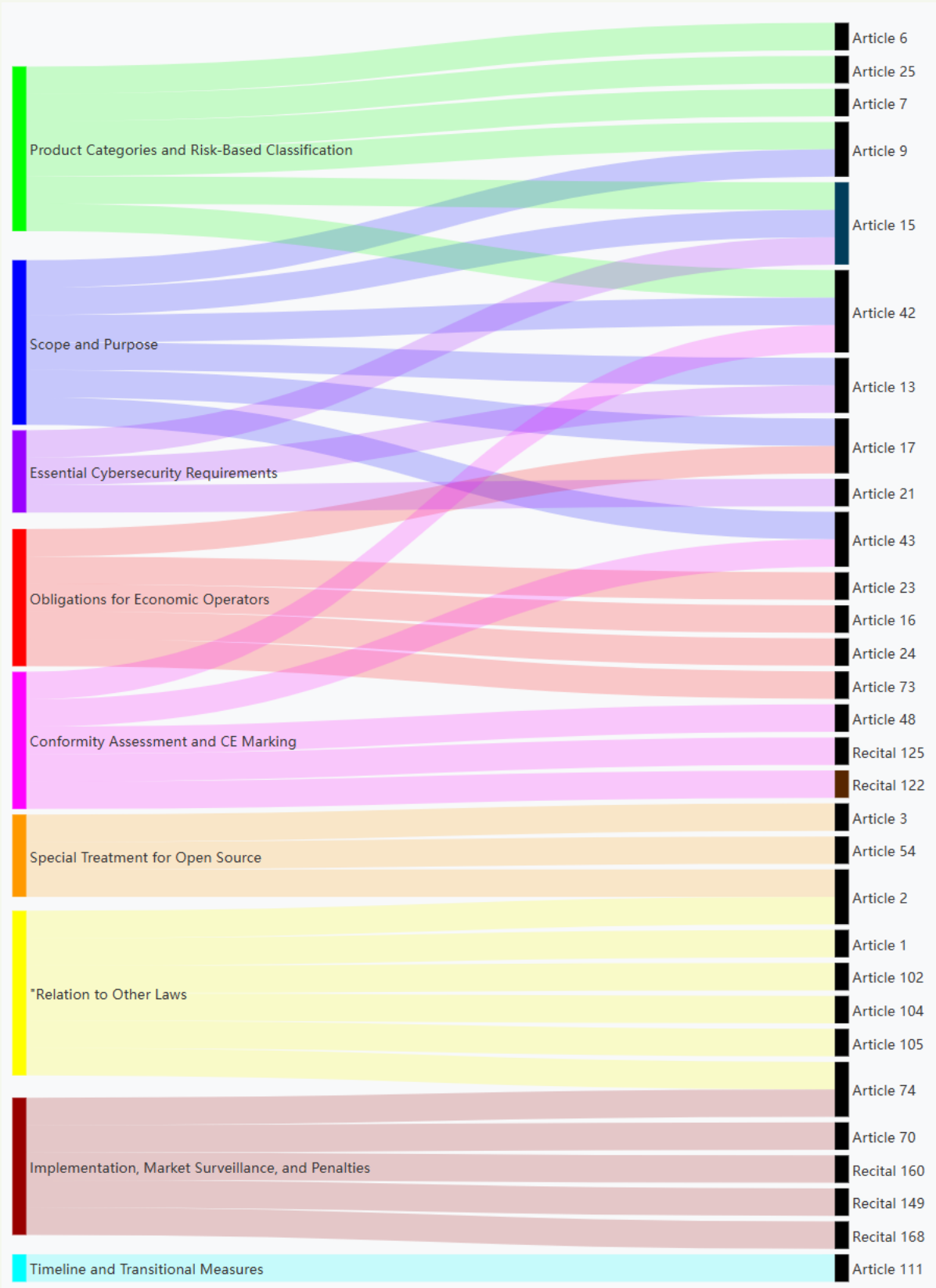
How does it work in practice?

Each EU Member State will designate market surveillance authorities responsible for checking compliance, investigating reported vulnerabilities, and conducting random inspections. Products found to be non-compliant may be recalled, removed from shelves, or prohibited from entering the market. Authorities can also issue administrative fines, which are defined in national legislation, based on the CRA's framework. Surveillance efforts are coordinated at the EU level via the ADCO group.

Mapping Cyber Resilience Act to EU AI Act

Cyber Resilience Act

EU AI Act



Cyber Resilience Act | EU AI Act

Section	Description	Provision(s)	Explanation	Action
Scope and Purpose	Covers all hardware and software with digital elements, including local and remote components. Aims to improve cybersecurity by mandating secure design and lifecycle practices to reduce vulnerabilities. Applies to manufacturers integrating cloud back-ends or services essential to product functionality.	15, 9, 42, 13, 17, 43	**Accuracy, Robustness, and Cybersecurity (Article 15)** • High-risk AI systems must be designed to achieve appropriate levels of accuracy, robustness, and cybersecurity throughout their lifecycle. This includes resilience against unauthorized alterations and measures to prevent data and model poisoning. **Risk Management System (Article 9)** • A continuous risk management process is required, addressing risks to health, safety, and fundamental rights. This includes evaluating risks from intended use and foreseeable misuse, and implementing mitigation measures. **Transparency and Information Provision (Article 13)** • High-risk AI systems must be transparent to enable deployers to interpret outputs appropriately. Instructions must	**Identify Covered Products and Components** Determine which hardware and software products fall under the CRA, including those with embedded or cloud-connected digital elements. Ensure your cybersecurity planning spans their entire lifecycle. **Determine high-risk status.** Obligations under the AI Act apply only if the product is regulated under a listed EU directive or regulation (Annex I) or performs a specifically listed high-risk use case. It is well possible that a product with digital elements under the CRA does not qualify as a high-risk AI system under the AI Act.

			include information on accuracy, robustness, and cybersecurity levels. **Quality Management System (Article 17)** • Providers must implement a quality management system to ensure compliance with the regulation, including aspects related to cybersecurity and risk management. **Conformity Assessment (Article 43)** • High-risk AI systems must undergo conformity assessments to ensure compliance with cybersecurity requirements. This may involve internal controls or assessments by notified bodies. **Presumption of Conformity (Article 42)** • AI systems certified under cybersecurity schemes are presumed to comply with the cybersecurity requirements of the Act.	
Product Categories and Risk-Based Classification	Covers all hardware and software with digital elements, including local	6, 25, 7, 9, 15, 42	**High-Risk AI Systems Classification (Article 6)** • AI systems are classified as high-risk if they are	**Classify Products by Risk Level** Assess and categorize products based on the listed legislation.

	and remote components. Aims to improve cybersecurity by mandating secure design and lifecycle practices to reduce vulnerabilities. Applies to manufacturers integrating cloud back-ends or services essential to product functionality.		intended to be used as safety components of products or are products themselves, covered by the Union harmonization legislation in Annex I. This is further limited to systems that require third-party conformity assessments. • AI systems are further classified as high-risk if they perform a use case listed in Annex III (and are not covered by the exception of article 6(3)). For products as meant under the CRA, this is rare but must be checked. **Amendments to High-Risk AI Systems (Article 7)** • The Commission can amend the list of high-risk AI systems by adding or modifying use-cases where AI systems pose a risk equivalent to or greater than those already listed. **Obligations of Providers and Deployers (Article 25)** • Providers and deployers of high-risk AI systems must ensure compliance with	Identify which products require third-party assessments and which can undergo internal evaluations. Determine the role of the AI: safety component or essential to the product? Evaluate the high-risk use cases of Annex III. Document these classifications to support compliance efforts.

			obligations, including specifying necessary information and technical access to enable compliance with the regulation. **Risk Management System (Article 9)** • A continuous risk management process is required for high-risk AI systems, addressing risks to health, safety, and fundamental rights, including cybersecurity risks. **Accuracy, Robustness, and Cybersecurity (Article 15)** • High-risk AI systems must be designed to achieve appropriate levels of accuracy, robustness, and cybersecurity throughout their lifecycle, including resilience against unauthorized alterations. **Presumption of Conformity (Article 42)** • AI systems certified under cybersecurity schemes are presumed to comply with the cybersecurity requirements of the Act.	

Obligations for Economic Operators	Manufacturers must assess risks, design secure systems, provide timely updates, and report incidents. Importers and distributors must ensure compliance before sale. Obligations cover product development, market release, and continued support throughout the defined product lifecycle.	17, 23, 16, 24, 73	**Manufacturers' Obligations** • **Risk Assessment and Secure Design**: Manufacturers, as providers of high-risk AI systems, must ensure compliance with the requirements set out in Chapter III Section 2, which includes conducting risk assessments and designing secure systems. • **Quality Management System**: Providers must implement a quality management system to ensure compliance with the regulation, which includes aspects related to risk management and cybersecurity. • **Incident Reporting**: Providers are required to report any serious incidents to the market surveillance authorities of the Member States where the incident occurred. **Importers' Obligations** • **Compliance Verification**: Before placing a high-risk AI	**Fulfill Manufacturer, Importer, and Distributor Duties** Ensure manufacturers build secure-by-design products and maintain update and incident response mechanisms. Importers and distributors must verify compliance before placing products on the EU market.

			system on the market, importers must ensure that the system complies with the regulation by verifying the conformity assessment, technical documentation, and CE marking. • **Information and Documentation**: Importers must provide competent authorities with all necessary information and documentation to demonstrate compliance and cooperate with authorities in any actions taken. **Distributors' Obligations** • **Pre-Market Compliance Check**: Distributors must verify that the high-risk AI system bears the required CE marking and is accompanied by the EU declaration of conformity before making it available on the market. • **Corrective Actions**: Distributors must take corrective actions if they consider or have reason to	

			consider that a high-risk AI system is not in conformity with the requirements.	
Essential Cybersecurity Requirements	Mandates secure-by-design principles, incident reporting, and coordinated vulnerability disclosure. Requires timely security updates, especially for consumer products, with opt-out for automatic updates. Transparency obligations include informing users about support periods, updates, and known risks.	15, 13, 21	**Secure-by-Design Principles (Article 15 AIA)** • High-risk AI systems must be designed and developed to achieve appropriate levels of accuracy, robustness, and cybersecurity throughout their lifecycle. This includes resilience against unauthorized alterations and measures to prevent data and model poisoning. **Incident Reporting (Article 14 CRA)** • Providers of high-risk AI systems are required to report cybersecurity incidents to the competent authorities. This ensures that any significant cybersecurity threats are promptly addressed. **AI-specific security measures (Article 15)** • The Act mandates technical solutions to address AI-specific vulnerabilities, including measures to	**Implement Core Cybersecurity Practices** Adopt secure development protocols, regular updates, and vulnerability management. Inform users about support periods, update policies, and potential cybersecurity risks in a transparent and accessible way.

			prevent, detect, respond to, and control attacks such as data poisoning and adversarial examples. **Timely Security Updates (Article 15 AIA, Annex I CRA)** • Providers must ensure that high-risk AI systems are updated to maintain cybersecurity. This includes providing timely updates, especially for consumer products, and allowing users to opt out of automatic updates. **Transparency Obligations (Article 13)** • High-risk AI systems must be accompanied by clear instructions that include information on the system's accuracy, robustness, and cybersecurity levels. Users must be informed about support periods, updates, and any known risks associated with the system.	
Conformity Assessment and CE Marking	Products must bear CE marking to show compliance. Most products can self-assess,	48, 43, 42, Recital 125, Recital 122	**CE Marking Requirements (Article 48)** • High-risk AI systems must bear the CE marking to	**Conduct Conformity Assessments and Affix CE Marking** Create internal or third-party evaluation processes to verify

	but Class II important and critical products need third-party evaluation. European cybersecurity certification schemes, like EUCC, may support or replace assessment in some cases.		indicate conformity with the EU AI Act. This marking should be affixed visibly, legibly, and indelibly on the system, its packaging, or accompanying documentation. **Conformity Assessment Procedures (Article 43)** • Providers of high-risk AI systems must follow specific conformity assessment procedures. These can include internal control or an assessment involving a notified body, particularly when harmonized standards are not applied or available. **Third-Party Evaluation (Recital 125)** • For certain high-risk AI systems, particularly those related to biometrics, a third-party conformity assessment involving notified bodies is required. This ensures a higher level of scrutiny and compliance. **European Cybersecurity Certification (Article 42)** • High-risk AI systems certified under European	compliance. For qualifying products, issue EU Declarations of Conformity and apply CE markings before placing them on the market.

			cybersecurity schemes, such as the EUCC, are presumed to comply with the cybersecurity requirements of the EU AI Act. This certification can support or replace the need for separate conformity assessments in some cases. **Presumption of Conformity (Recital 55)** • AI systems that have been certified under a cybersecurity scheme are presumed to comply with the cybersecurity requirements of the EU AI Act, provided the certification covers those requirements.	
Special Treatment for Open Source	Non-commercial FOSS is exempt. Commercial use of FOSS is included. A light regulatory regime applies to open-source stewards like foundations providing sustained development or infrastructure. This supports innovation while ensuring accountability for widely-used	2, 3, 54	**Exemption for Non-Commercial FOSS (Article 2)** • The EU AI Act does not apply to AI systems released under free and open-source licenses unless they are placed on the market or put into service as high-risk AI systems or fall under specific prohibitions. **Inclusion of Commercial Use of FOSS (Article 3)**	**Manage Open Source Responsibly** Inventory all open-source software used. Ensure commercially used OSS components meet CRA standards. For widely used OSS, apply appropriate oversight and update strategies to mitigate vulnerabilities.

	software components.		• Providers of general-purpose AI models, including those released under open-source licenses, are subject to the regulation if they present systemic risks or are used commercially. This ensures that commercial applications of FOSS are included under the regulatory framework. **Light Regulatory Regime for Open-Source Stewards (Article 54)** • Open-source stewards, such as foundations that provide sustained development or infrastructure, are encouraged to participate in the regulatory framework. This supports innovation while ensuring accountability for widely-used software components.	
Relation to Other Laws	Aligns with NIS2, AI Act, GDPR, and product-specific regulations. Ensures harmonization without overlap. Sector-specific rules may override the CRA if they offer equal or stronger	2, 1, 74, 102, 104, 105	**Harmonization with Existing Regulations (Article 1)** • The EU AI Act aims to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy AI	**Align with Other EU Laws and Directives** Map CRA obligations against EU AI Act, GDPR, NIS2, and other applicable laws. Coordinate legal and technical teams to ensure consistent, cross-regulation cybersecurity compliance

	protection. The regulation integrates into the broader EU cybersecurity and safety framework.		while ensuring a high level of protection for health, safety, and fundamental rights. It is designed to harmonize with existing EU laws, including those related to consumer protection and product safety. **Non-Overlap with GDPR (Article 2)** • The Act explicitly states that it does not affect the application of Union law on the protection of personal data, such as GDPR. This ensures that AI systems comply with data protection regulations without overlap. **Sector-Specific Regulations (Article 2)** • The Act does not apply to AI systems used exclusively for military, defense, or national security purposes, nor does it affect the competences of Member States concerning national security. This allows sector-specific rules to take precedence where they offer	throughout your business processes

			equal or stronger protection. **Integration into EU Cybersecurity Framework (Article 74)** • The Act aligns with the broader EU cybersecurity framework by applying Regulation (EU) 2019/1020 to AI systems, ensuring effective market surveillance and control. This integration supports harmonization across different regulatory areas. **Amendments to Existing Regulations (Articles 102, 104, 105)** • The Act includes amendments to existing regulations, such as Regulation (EC) No 300/2008 and Directive 2014/90/EU, to ensure that AI systems comply with safety and security requirements set out in the AI Act.	
Timeline and Transitional Measures	Products on the market before application are exempt unless significantly changed. A transitional period, likely three years, allows time for adaptation. This phased approach helps businesses,	111	**Exemption for Existing Products (Article 111)** • AI systems that are components of large-scale IT systems placed on the market before August 2, 2027, must comply with the regulation by December 31, 2030. For other	**Prepare for the Transition Period** Start a compliance gap analysis now. Develop a timeline and roadmap aligned to the CRA's transition period. Train key teams and prioritize product updates to avoid future disruptions.

	especially SMEs, prepare for compliance without disrupting current operations.		high-risk AI systems placed on the market before August 2, 2026, the regulation applies only if there are significant changes in their design after that date. **Transitional Period for Compliance** • Providers of general-purpose AI models placed on the market before August 2, 2025, must comply with the regulation by August 2, 2027. This phased approach allows businesses, particularly SMEs, to adapt to the new requirements without disrupting current operations.	
Implementation, Market Surveillance, and Penalties	National authorities ensure compliance through inspections and coordination via the ADCO group. SBOMs support dependency assessments. Penalties for non-compliance include product recalls, market bans, and fines. Focus on proactive enforcement and	70, 74, Recital 160, Recital 149, Recital 168	**Role of National Authorities and Coordination (Article 70)** • Each Member State is required to designate national competent authorities, including market surveillance authorities, to ensure compliance with the EU AI Act. These authorities must operate independently and impartially to	**Establish Compliance Monitoring and Response Systems** Set up internal compliance teams, maintain complete SBOMs, and prepare for inspections. Create action plans for addressing non-compliance, including recall and market withdrawal protocols.

	improved cybersecurity situational awareness across the EU.		safeguard the objectivity of their activities. **Coordination via the ADCO Group (Recital 46)** • The European Artificial Intelligence Board is responsible for facilitating coordination among market surveillance authorities through the Administrative Cooperation Group (ADCO). This group acts as a platform for cooperation and exchange on market surveillance issues. **Market Surveillance and Inspections (Article 74)** • Market surveillance authorities are empowered to conduct inspections and enforce compliance with the EU AI Act. They have the authority to propose joint activities, including joint investigations, to promote compliance and identify non-compliance. **Penalties for Non-Compliance (Recital 168)** • Member States are required to implement	

			effective, proportionate, and dissuasive penalties for non-compliance with the EU AI Act. These penalties can include product recalls, market bans, and fines. The European Data Protection Supervisor has the power to impose fines on Union institutions, agencies, and bodies. **Proactive Enforcement and Cybersecurity Awareness (Recital 160)** • The EU AI Act emphasizes proactive enforcement and improved cybersecurity situational awareness across the EU. Market surveillance authorities and the Commission can propose joint activities to enhance compliance and raise awareness about cybersecurity risks.	

Calls to action

Integrate CRA Secure-by-Design Principles into AI Development Lifecycles

The EU AI Act mandates that high-risk AI systems be secure, robust, and resilient against cyber threats. By embedding the CRA's secure-by-design obligations—such as risk-based threat modelling, lifecycle security support, and vulnerability patching—into your AI development lifecycle, you can meet these cybersecurity requirements proactively while building products that are safer and more resilient from day one.

Use CRA Conformity Assessments to Streamline AI CE Marking

High-risk AI systems under the AI Act must undergo conformity assessments and display CE marking. CRA-certified digital products already meet baseline cybersecurity requirements and may benefit from the AI Act's presumption of conformity. Organizations can accelerate compliance by aligning AI conformity workflows with existing CRA assessment procedures and leveraging shared documentation, technical files, and test results.

Establish Coordinated Incident and Vulnerability Disclosure Protocols

Both the AI Act and CRA require incident reporting and vulnerability management. Organizations should create unified procedures for disclosing cybersecurity incidents across AI and non-AI products, integrating CRA obligations (e.g., timeline and authority notification) with the AI Act's requirements for high-risk system incident response. This reduces compliance complexity and enhances regulatory readiness.

Leverage CRA Risk Classification to Support AI Risk Management Systems

The AI Act requires continuous risk management for high-risk systems. The CRA's tiered product risk classification—general, important, and critical—offers a practical starting point for identifying system-level cybersecurity exposure. By mapping CRA product risk classes to AI system risk assessments, organizations can align controls, prioritize mitigation, and justify proportional safeguards under both regulations.

Conclusion

The convergence of the EU Cyber Resilience Act (CRA) and the EU Artificial Intelligence Act (AI Act) marks a significant evolution in Europe's digital governance—reflecting a shared commitment to secure, trustworthy, and risk-aware development of intelligent technologies. As digital products increasingly integrate AI and shape critical infrastructure, aligning cybersecurity regulation with AI-specific governance is essential to fostering resilience, accountability, and legal certainty across the EU single market.

This mapping report highlights the complementary strengths of both frameworks. The CRA offers a lifecycle-oriented, product-level cybersecurity regime, mandating secure-by-design principles and vulnerability management across all hardware and software with digital elements. Meanwhile, the AI Act introduces a risk-based framework for high-risk AI systems—anchored in human oversight, transparency, and fundamental rights protections. Together, these laws create a robust ecosystem for regulating intelligent digital systems—reinforcing core pillars such as secure innovation, market surveillance, quality assurance, and cross-sector accountability.

Achieving the full benefits of this convergence depends on how effectively organizations integrate CRA cybersecurity requirements into AI development pipelines. This means translating AI Act provisions—like conformity assessments and risk management systems—into operational practices that also meet CRA obligations for vulnerability disclosure, CE marking, and incident reporting. It also demands coordinated governance across legal, technical, and product teams.

Despite their differing scopes, early alignment between the CRA and AI Act already demonstrates practical benefits: improved security posture for AI-enabled products, reduced duplication of compliance efforts, and smoother conformity procedures for high-risk AI systems. As AI becomes increasingly embedded in connected products and critical services, the co-regulation introduced by these two Acts offers a unified path toward building digital technologies that are not only innovative and competitive, but also secure, explainable, and legally compliant by design.

Authors

Arnoud Engelfriet

Chief Knowledge Officer at ICTRecht

"The AI Act and Cyber Resilience Act show how deeply technical the law has become. Behind every CE mark and compliance checklist lies a web of risk models, lifecycle security dependencies, and engineering trade-offs. Lawyers and engineers must now collaborate to make these frameworks workable in practice.

"At their heart, both Acts are structured risk management systems. They embed accountability and resilience into every layer of digital products and AI systems, turning abstract legal principles into practical obligations that shape how technology is designed, built, and maintained."

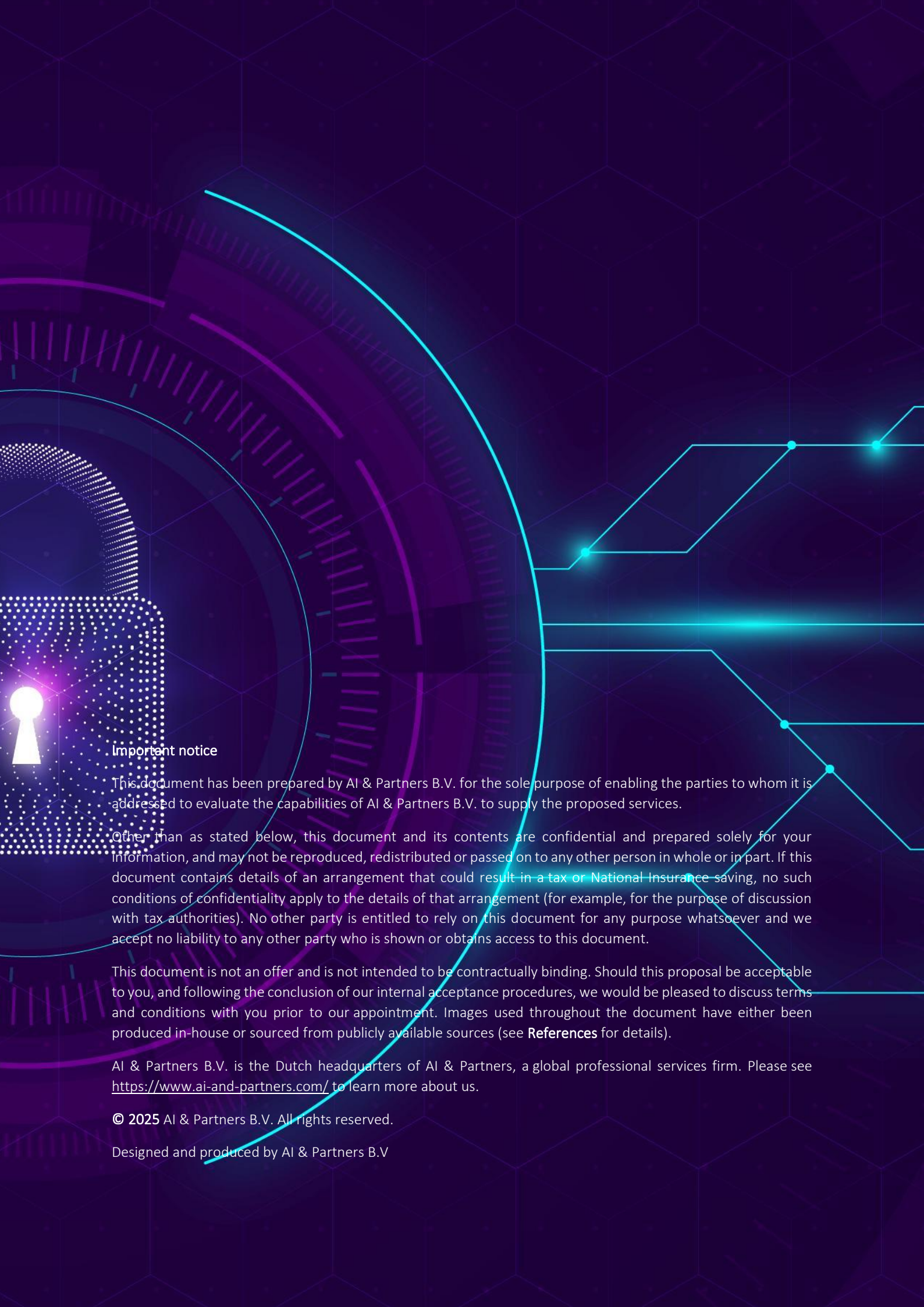
Biography

Arnoud Engelfriet is a Dutch IT lawyer and computer scientist, serving as Chief Knowledge Officer at the legal services firm ICTRecht in Amsterdam. He specializes in AI, data and software, and enjoys delving into complex challenges at the intersection of ICT and law, a subject he has been blogging about every working day since 2007. He is a much sought-after speaker, author of books and guest lecturer. His latest books AnnotatedAIAct.com and AI and Algorithms show the legal and technical developments in ICT law that culminated in the AI innovation revolution in which we find ourselves today. Arnoud took the initiative to create the certified "CAICO®" course for AI Compliance Officers.

References

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 13th June 2025)

European Parliament and The Council of the European Union, (2024), Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance), accessible at https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (last accessed 13th June 2025)



Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V