EU Cyber Resilience Act: 101

By Cheryl Saniuk-Heinig and Ana Bruder

Purpose of the Cyber Resilience Act	Key changes the Cyber Resilience Act will bring	Key challenges posed by the Cyber Resilience Act
→ Establishes uniform cybersecurity requirements for products with digital elements across the EU → Seeks to enhance the internal market's functioning and ensure a high level of cybersecurity through secure products by harmonizing requirements and complementing the NIS2 cybersecurity framework	→ Establishes cybersecurity requirements for products with digital elements, which need to be designed, developed and maintained to mitigate cybersecurity risks → Requires manufacturers to identify and remediate vulnerabilities contained in the product, including by providing security updates, and to publicly disclose information about fixed vulnerabilities → Requires manufacturers to consider cybersecurity throughout a product's life cycle → Introduces enhanced market surveillance mechanisms relying on conformity assessments, European cybersecurity certifications and harmonized standards to ensure compliance with cybersecurity requirements	→ Achieving compliance across diverse range of products. → Understanding the interplay with other EU laws, such as the AI Act, Data Act, GDPR, NIS2 Directive and Digital Operational Resilience Act.

FOCUS AREAS	CYBER RESILIENCE ACT
ENTITIES WITHIN SCOPE	The CRA applies to: → Manufacturers, developers, importers and distributors of products with digital elements, meaning hardware and software placed or made available on the EU market (which means supplied for distribution or use). → Manufacturers or developers of components of products with digital elements, which may constitute products with digital elements falling under the CRA. → Open-source software suppliers, but only when software is developed or supplied in a commercial context.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Published September 2025.
iapp.org

FOCUS AREAS	CYBER RESILIENCE ACT
COVERED PRODUCTS	The CRA applies to all products with digital elements, including: → Consumer electronics: Smartphones, laptops, smart home devices, wearables and connected appliances. → Industrial and critical infrastructure components: Routers, Internet of Things devices, control systems and industrial software. → Software solutions: Operating systems, mobile apps, application software, development libraries and firmware. → Cybersecurity software: Identity management and privileged access management software, firewalls and intrusion detection systems.
	Exemptions include: → Products already covered by specified product safety legislation, such as medical and in vitro diagnostic devices, radio equipment, civil aviation, marine equipment and vehicles. → Products with digital elements that are developed or modified exclusively for national security or defense purposes. → Spare parts to replace identical components and follow the same specifications as the components they are intended to replace.
TECHNICAL SECURITY REQUIREMENTS FOR COVERED PRODUCTS	Manufacturers determine the appropriate control mechanisms necessary to ensure protection from unauthorized access, which may include: → Secure authentication mechanisms, such as multifactor authentication or cryptographic key management. → Encrypted data transmission using industry-standard protocols. → Secure boot mechanisms to prevent unauthorized firmware modifications. → Logging and monitoring capabilities for security incident detection. → Sandboxing and privilege separation to prevent lateral movement.
SECURITY AND INCIDENT HANDLING OBLIGATIONS	The CRA has mandatory reporting requirements. Manufacturers must: → Report actively exploited vulnerabilities or severe incidents having an impact on the security of a product without undue delay and within 24 hours in addition to follow-up notices. → Notify impacted users of the product with digital elements.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

FOCUS AREAS	CYBER RESILIENCE ACT		
	Security by design and default	**Risk categorization of products**	**Impact on businesses and consumers**
KEY REQUIREMENTS	→ Integrate cybersecurity from the product's initial design phase. → Ensure secure default configurations, disabling unnecessary features and open ports. → Ensure that vulnerabilities can be addressed through security updates. → Ensure protection from unauthorized access through appropriate control mechanisms. → Employ secure software development life cycle principles, including static and dynamic code analysis, secure coding guidelines such as Open Worldwide Application Security Project and the National Institute of Standards and Technology. → Regular testing, including vulnerability scanning and penetration testing, and vulnerability handling including disclosures.	The CRA introduces a risk-based classification system for products: → All products are subject to baseline security requirements and conformity assessments, which include an internal control conformity assessment. → Critical products that present a critical level of cybersecurity risk are subject to requirement to obtain a European cybersecurity certification with an assurance level of at least "substantial." → Important products present a higher cybersecurity risk than other products with digital elements. Important products that fall under Class II should always involve a third-party assessment, including a European cybersecurity certification with an assurance level of "substantial," when available. Important products in Class I will only require a third-party conformity assessment if they do not meet the harmonized standards or do not have an European cybersecurity certification at “substantial” assurance level. • Class I includes identity management systems, VPNs, security information and event management systems, password managers, network management systems, operating systems, routers, microprocessors and microcontrollers with security-related functions, certain smart home virtual assistants and products, internet-connected toys and personal wearable devices. • Class II includes certain hypervisors and container runtime systems, firewalls, intrusion detection or prevention systems and tamper-resistant microprocessors and microcontrollers.	→ Increased compliance costs for cybersecurity assessments, vulnerability handling, certifications and reporting. → Market access barriers for products that are not CRA-compliant as both importers and distributors are obliged to ensure the products with digital elements that they buy and sell have the CE marking. → A CE marking (Conformité Européene or European Conformity marking) represents a manufacturer's declaration that products comply with EU rules relating to safety, health, environmental protection--and now cybersecurity.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

FOCUS AREAS	CYBER RESILIENCE ACT
ENFORCEMENT AND PENALTIES	Noncompliance penalties include: → Fine for failing to meet cybersecurity requirements and reporting obligations: 15 million euros or 2.5% of global annual turnover, whichever is higher. → Fine for failure of other specified obligations, such as relating to declaration of conformity, technical documentation or failure to provide access to data: 10 million euros or 2% of global annual turnover, whichever is higher. → Fine for supplying incorrect, incomplete or misleading information to conformity assessment bodies and market surveillance authorities: 5 million euros or 1% of global annual turnover, whichever is higher. → Market withdrawal orders by national competent authorities for products failing to meet security standards. → Temporary or permanent bans by national competent authorities on noncompliant products. → Potential liability for damages caused by cybersecurity failures under the laws of the EU member states. Consistent with the principle established in Directive (EU) 2024/2853, manufacturer liability may be triggered where a lack of safety consists in the lack of security updates after the placing of the product on the market, and this causes damage.
IMPORTANT DATES	→ 10 Dec. 2024: Entry into force of the CRA, marking the beginning of the implementation period. → 2024-27: EU institutions to develop detailed guidelines and enforcement mechanisms. → 11 June 2026: Conformity assessment bodies established and Chapter IV takes effect. → 11 Sept. 2026: Manufacturer reporting obligations for actively exploited vulnerabilities and severe incidents impacting product security, as outlined in Art. 14, take effect. → 11 Dec. 2027: CRA becomes fully applicable.

Additional resources

→ EU Cyber Resilience Act official text → Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis | ENISA

→ What to know about the EU Cyber Resilience Act | IAPP → Navigating the new EU cybersecurity standards: The NIS2 Directive and Cyber Resilience Act | IAPP

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.