EU CYBER RESILIENCE ACT
FREQUENTLY ASKED QUESTIONS

The Cyber Resilience Act (CRA) is European Union (EU) legislation that introduces cybersecurity rules that apply to manufacturers, importers, and distributors of products with digital elements, and it covers both hardware and software.

The CRA received formal approval by the European Parliament in March 2024 and was adopted by the European Council on October 10, 2024. It was published in the EU Official Journal on November 20, 2024 and will enter into force on December 10, 2024. Most of its requirements will be fully applicable on December 11, 2027.

1 What is the objective of the Cyber Resilience Act?

The Cyber Resilience Act is intended to ensure that:

- Wired and wireless products that are connected to the internet and software placed on the EU market are more secure.
- Manufacturers remain responsible for a product's cybersecurity throughout its lifecycle.
- Consumers are properly informed about the cybersecurity of products they buy and use.

>> See the EU's FAQ.

2 What does the CRA regulate?

The CRA applies to "products with digital elements" (PDEs) that are commercially available in the EU, regardless of place of manufacture. PDEs include standalone software, products with both software and hardware that have a direct or indirect connection to a device or network (such as IoT devices), and software and hardware components that are integrated into PDEs.

The CRA does not apply to everyone. It excludes websites and cloud applications that do not support remote processing or functionality for a PDE, open source software developed outside of commercial activity, or products covered by other sectoral EU regulation (such as medical devices, motor vehicles, or maritime/ aeronautical equipment).

The CRA imposes cybersecurity requirements for PDEs, with its core obligations imposed on PDE manufacturers. One notable requirement is that manufacturers must ensure that their products adhere to the appropriate levels of cybersecurity based on various PDE risk categories, with more intensive conformity assessments required for PDEs associated with higher risk levels.

The CRA sets three PDE categories (or four, depending on how you want to count):

IMPORTANT (CLASS I AND CLASS II)
The Important PDE is separated into two classes:

PDEs categorized into Classes I and II meet specific criteria:

- **Class I:** The product primarily performs functions critical to the cybersecurity of other products, networks, or services, including securing authentication and access, intrusion prevention and detection, endpoint security, or network protection.
- **Class II:** The product performs a function that carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control, or cause damage to a large number of other products or to the health, security, or safety of its users through direct manipulation. One example is a central system function, including network management, configuration control, virtualization, or processing of personal data.

CRITICAL

PDEs in the CRA's Critical cybersecurity category must conform with a cybersecurity certification scheme relevant to the PDE's product type. These add two additional criteria to the "Important" product class:

- **The critical dependency of essential entities:** This is discussed in Article 3 of Directive (EU) 2022/2555 — a.k.a. NIS2 — on the category of products with digital elements. More simply put, these products protect essential entities whose failure could have systemic effects within the EU, such as actors in the transport, energy, or health sectors. More detail about Essential Entities (EEs) is in the NIS2 compliance guide.
- **Their effect on the supply chain:** The certification is labeled as critical when the PDEs' incidents and exploited vulnerabilities can lead to serious disruptions to critical supply chains across the internal market. More simply put, these products are critical to the extent that they secure the supply chain.

DEFAULT CATEGORY

The Default category applies to other products that do not fall under the Important Class I, Important Class II, or Critical categories. They should comply to CRA through self-assessment.

3 When will the CRA take effect?

The CRA was approved by the European Parliament in March 2024 and by the European Council in October 2024. It was published in the EU Official Journal on November 20, 2024 and to go into effect on December 10, 2024. It has a 36-month implementation timeline with most of its requirements being fully applicable on December 11, 2027.

Two exceptions fall within the 36-month deadline:

- Manufacturers must implement the security vulnerability and cyber incident reporting obligations within 21 months.
- Conformity assessment bodies must be established within 18 months. (This only applies to auditors.)

4 What timelines does the CRA set for reporting severe incidents and exploitable vulnerabilities?

The CRA defines a severe incident as an incident wherein:

- The ability of the product to protect the availability, authenticity, integrity, or confidentiality of sensitive information is compromised.
- Malicious code has been introduced into the PDE and can be executed.

An active exploitable vulnerability, as defined by the CRA, is a system vulnerability that a malicious actor exploited (based on reliable evidence) without permission of the system owner.

According to the CRA, PDE manufacturers, importers, and distributors are obligated to report severe incidents and exploitable vulnerabilities to the proper authorities. In this case, the authorities are the European Union for Cybersecurity (ENISA) and Computer Security Incident Response Team (CSIRT).

- ENISA is an agency equivalent to the US Government's Cybersecurity Infrastructure and Security Agency (CISA). ENISA helps the EU and its member states prepare for, detect, and respond to information security issues. It also contributes to the EU's cybersecurity policy.
- As defined by the CRA, CSIRT is designated by EU member states to coordinate and respond to cybersecurity incidents. It also provides cybersecurity expertise.

In the event of a severe incident or active exploitable vulnerability, the PDE manufacturer must:

- Provide an early warning notification to the CSIRT and ENISA within 24 hours of awareness, outlining whether the incident is suspected to have been caused by a malicious/unlawful act and noting in which EU countries the PDE is available.
- Provide a second notification to those agencies no later than 72 hours from awareness, with relevant information (unless already provided), such as the nature of the incident/vulnerability or an initial assessment and any mitigation measures.

- For a severe incident, the PDE manufacturer must provide the EU agencies with a report within one month of the previous notification, unless all relevant information was already provided. The report should include:
  - A description of the incident, with severity and impact analysis
  - The root cause of the threat
  - Mitigation
- For an active exploitable vulnerability, a final report, made no later than 14 days after corrective or mitigating measures (patches) have been made available, must include:
  - A description of the vulnerability, with a severity and impact analysis
  - If available, information about any malicious actor exploiting the vulnerability
  - Security updates and other mitigations for the vulnerability

5 To which standards does the CRA align?

ENISA published a CRA Requirements Standards Mapping, which shows how the CRA requirements map to multiple international standards, including the ISO-27000 series and IEC 62443. In that mapping is a gap analysis and best-practices recommendations in comparison with other standards, such as NIST special publications pertaining to cybersecurity and information security.

In addition, the US-EU Cyber Dialogue held in December 2023 was aimed at facilitating mutual recognition of certifications between the US Cyber Trust Mark program and the EU's CRA. If this recognition is successful, certain US product security standards may satisfy the CRA requirements.

6 What are the penalties when CRA-regulated products fail to comply with CRA regulations?

Failure to comply with vulnerability reporting, cyber incident reporting, or essential cybersecurity requirements could trigger administrative fines of up to €15 million or 2.5% of global turnover. Other obligations include €10 million or 2% of global turnover.

7 What is the correlation between the CRA and NIS2 EU-wide cybersecurity directives?

Network Information Security (NIS2) will replace a previous directive, NIS, which is EU-wide cybersecurity legislation. While the CRA covers cybersecurity for products, NIS2 requires organizations in specific industries to ensure that networks and information systems have the proper security controls to tackle cyberattacks.

8 How will Wind River comply with the CRA?

Naturally, industry players are planning ahead to ensure compliance with the CRA — including Wind River®.

Wind River is closely tracking the CRA's progress. We are considering how it applies to the Wind River edge and platform products both to ensure regulatory compliance and to further our commitment to product security.

Wind River products already conform to the NIST Secure Software Development Framework (SSDF), particularly in regard to the secure development lifecycle. There are alignments between the CRA security requirements and the NIST SSDF.

Wind River's Professional Services team works with customers to support their compliance and certification activities, including any gap and security assessments. As a vendor and software supplier to OEMs, Wind River has performed certification activities for numerous industry standards, including those of NIST, ISO/IEC, DOD, and FDA.

As part of compliance and certification activities, Wind River provides its customers with important documentation and artifacts that are used as evidence for third-party assessors and certifying agencies. Some examples of these documents and artifacts include (but are not limited to):

- Secure Development Lifecycle Standards Mapping www.windriver.com/resource/sdl-standards-map
- ISO 27001 Information Security Management, which demonstrates Wind River's commitment and ability

to manage information securely and safely www.windriver.com/resource/iso27001

- Product Security Incident Response Team (PSIRT) aligns ISO/IEC 30111 (IT security techniques, vulnerability handling, and process) and ISO/IEC 29147 International Standards, providing guidelines for vulnerability disclosure www.windriver.com/security#psirt

9 Do Wind River products adhere to "secure by design" as it pertains to the CRA core principles?

Wind River Edge products — VxWorks®, Wind River Linux, and Wind River Helix™ Virtualization Platform — comply with NIST 800-218 SSDF, which addresses a set of requirements that produces secure software.

>> Consult this description of our secure development lifecycle directly aligned to SSDF.

10 How does Wind River help customers with the CRA?

Wind River has been delivering value-driven solutions with its edge products for more than 40 years. These solutions include support from Wind River Professional Services, which provides expertise regarding activities related to security assessments, security gap analysis, and security certification for a variety of industry standards, frameworks, and guidelines — not just this one.

IEC 62443, a set of security standards for the secure development of industrial automation and controls systems (IACS), plays a key role for the CRA. VxWorks Cert Edition is certified to GE Digital Achilles Level II for compliance to IEC 62443-4-2. IEC 62443-4-2 specifies security requirements such as physical security, network communications security, and secure systems integration. With VxWorks Cert Edition, Wind River customers can be assured that the product has passed rigorous cybersecurity testing to meet the requirements set forth by the IEC 62443-4-2 standard and protect against cybersecurity threats for IACS.

>> Explore Wind River's involvement in industrial standards.

11 How does Wind River help customers solve CRA compliance challenges?

Wind River develops products based on the NIST Secure Software Development Framework, and the website discusses Wind River's secure development lifecycle.

NIST SP 800-218 Secure Software Development Framework (SSDF) provides fundamentals for the secure development of software products. These best practices align and map to various compliance standards such as IEC 62443. Wind River can provide that mapping to our customers and engage on next steps to cover any security requirement gaps.

Wind River Professional Services brings to bear vast experience in security assessments that help our customers cover unique security requirements and gaps that our products do not explicitly cover.

12 What additional products and services can Wind River provide to help our customers adhere to the CRA?

VxWorks, Helix Platform, and Wind River Linux OS adhere to NIST SSDF. This framework aligns to security guidelines such as IEC 62443 for IACS, which plays a key role in achieving the CRA objectives.

One CRA element is the delivery of a software bill of materials (SBOM), with digital elements along with the proper management of software vulnerabilities. Wind River offers both paid and free SBOM generation tools and an online CVE scanning tool.

>> Explore Wind River Studio Linux Services, the free open source SBOM Yocto layer for Wind River Linux builds, and the CVE scanning tool.