

# Does the EU CRA affect my business?

Mike Bursell, Co-chair, OpenSSF Cyber Policy WG

*This guide is not intended to provide legal advice and we encourage you to seek advice from your legal counsel if you should run into any issues or have any questions. Such a determination likely requires consulting with a legal counsel or your employer's legal team.*

## Introduction

**The European Union's Cyber Resilience Act (CRA) is a piece of legislation that covers all countries within the EU and the EEA and entered into force on 10th December 2024. It covers many types of devices and applications that are either sold or otherwise made commercially available on the European market and the intention behind it is to improve the cybersecurity of products available to consumers and businesses across Europe.**

This article looks at the CRA and whether it is likely to affect your business or product and is a companion to the article “**What do I need to do for the EU**

**CRA?”** The details of implementation of the CRA are still being worked out and although most of the measures aren't due to come into force until November 2026, the impact of the Act is going to be wide-ranging. For many organisations and businesses, there will be important changes to processes around how they create, document, sell, upgrade and support products, all of which require planning and implementation well in advance of full implementation of the Act. While this article should not be considered as providing legal advice, it will give you basic information to allow you to decide next steps.

Some commentators have seen the CRA as imposing a new burden of cybersecurity awareness on organisations. However, the view of many cybersecurity professionals, and that of the Linux Foundation and the OpenSSF, is that it actually **presents an opportunity to normalise cybersecurity as a part of all organisations** and to raise the visibility of security practices throughout the supply chain and lifecycle of all products. This provides a chance for industry to get to grips with a subject that has long been neglected and to work to provide standards, tools and techniques that will benefit the entire ecosystem, similar to the changes that have been put in place around privacy to satisfy the requirements around GDPR.

**The first thing to work out is whether you are likely to be affected.**

Do you produce a PDE?

The CRA applies to what are defined as **Products with Digital Elements** (PDEs). A PDE is defined as “a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.”

This definition covers a wide range of products and services and **it's important to note that if your product requires access to an online service (for example, a back-end API) in order to function, that's likely to be covered as well, whether it's hosted in the EU or not.** A stand-alone website is unlikely to fall within the CRA and there are some specific sectors (such as telecommunications, healthcare and automotive) which, while subject to the CRA already

have conformity requirements applied to them. **If you produce a PDE, you are likely to be what the CRA calls a “Manufacturer”, which imposes specific requirements on you and how you bring your PDEs to the EU marketplace.**

Examples might include: an Internet connected dishwasher, business software that users or administrators install on their PCs; a packaged mobile app that provides an AI chat assistant; a fitness tracking watch.

Do you do business in Europe?

**If your product is sold or “offered” in the EU, or you make a profit from it in some way, then this means that it is likely to be subject to the CRA.**

The good news, however, is that the CRA is designed to be consistent across the EU, so if you have achieved compliance in one part of the EU, that covers all other member countries as well. It's worth noting that “small and medium-sized enterprises” (SMEs) are subject to slightly reduced requirements under the CRA. Proof of Concept and Beta products are generally exempt from the CRA.

## Open Source

One of the important features of the CRA is its awareness of open source and the ecosystem around it. It introduces the term (and role) “Steward”, used to refer to entities such as open source software foundations that don’t sell PDEs, but do manage, support,

publish and host open source projects. **The CRA imposes fewer and less onerous requirements on Stewards than on Manufacturers**, though they do have responsibilities for working

with maintainers and contributors of open source on the one hand and manufacturers on the other. **The CRA is also aware of the role of**

**maintainers and contributors. They are not affected directly by the CRA**, particularly if the project on which

they are working is supported by a Steward, though if they make a profit from services around the project, they may count as a Manufacturer. It is also possible for an organisation to be both a Manufacturer and a Steward: if the organisation both sells a PDE that uses an open source project and also hosts it, supports it and provides updates and patches for the community, for instance, then that would put it in both categories. And it’s important to note that open source projects do not necessarily need to have a Steward at all.

## Finding out more

The Linux Foundation Europe and OpenSSF invite the broader open source community to participate in this initiative. To get involved:

- Visit the WG Repository: [Global Cyber Policy WG GitHub](#)
- Join Our Slack Channel: [#wg-globalcyberpolicy on Slack](#)
- Subscribe to Mailing Lists:
  - [Global Cyber Policy WG Mailing List](#)
  - [CRA Readiness+Awareness SIG Mailing List](#)
  - [CRA Tooling+Process+Formats SIG Mailing List](#)
  - [CRA Spec Standardization SIG Mailing List](#)

# What will my business need to do for the EU CRA?

Mike Bursell, Co-chair, OpenSSF Cyber Policy WG  
January 2025

## Introduction

The European Union's Cyber Resilience Act (CRA) is a piece of legislation that covers all countries within the EU and the EEA and entered into force on 10th December 2024. It covers many types of devices and applications that are either sold or otherwise made commercially available in Europe and the intention behind it is to improve the cybersecurity of products available to consumers and businesses across Europe.

This article looks at the CRA and how it is likely to affect your business, and is a companion to the article "[Does the EU CRA affect my business?](#)". Note that the requirements on "open source stewards" are different, and not covered within this article. The details of implementation of the CRA are still being worked out and although most of the measures aren't due to come into force until September 2026, the impact of the Act is going to be wide-ranging. For many organisations and businesses, there will be important changes to processes around how they create, document, sell, upgrade and support products, all of which require planning and implementation well in advance of full implementation of the Act. While this article should not be considered as providing legal advice, it will give you basic information to allow you to decide next steps.

## Compliance and conformity

The CRA applies to what are defined as **Products with Digital Elements** (PDEs). A PDE is defined as "a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately."

**Core to the CRA is a requirement that most PDEs will be required to be conformant with the Act, and extends the "CE mark" to PDEs.** In some cases, conformity can be demonstrated through following particular processes and declaring that your PDE meets the specific requirements (though this may be checked by another agency); this is known as "internal conformance based on internal control" and still requires notification to an appropriate EU body. In other cases the PDE must be

**submitted for external assessment** by an organisation or individual authorised by the EU. It is expected that cross-certifications (by equivalent bodies in other jurisdictions) will be accepted in the future. Which PDEs fit into which classes, and therefore require what - and levels - of conformity has been specified, and a fuller definition should be available by December 2025.

Some of the classification types are discussed in the [Classes of PDEs](#) below.

**Compliance is a wider concept, which starts with having a PDE that conforms to the requirements, but involves a continuing set of actions such as vulnerability management. The most important of these are listed under [Compliance measures](#).**

### Classes of PDEs

Some types of PDEs are already covered by EU legislation, including many of those used in telecommunications, healthcare and automotive sectors, as well as those used for national security or defence, are not covered by the CRA. Other types of PDEs are listed below, with the expected requirements for conformity.

- **Important PDEs - PDEs that have a high risk in that they might have a negative impact on the health, security or safety of users if they malfunctioned or were compromised will be classified as “important PDEs”.** There are **two** categories of important PDEs: **Class I & Class II, with Class II having a higher possible impact** (see CRA Annex III). These are required to undergo external conformity assessment. Important PDEs include Operating Systems, routers, health monitoring wearables, browsers, virus scanners, baby monitors, firewalls and much more.
- **Critical PDEs - PDEs that have a specific cybersecurity function (see CRA Annex IV).**

These are required to undergo external conformity assessment - these include devices like smart electricity meters or smart cards.

- **Open source PDEs** - PDEs that are **100% open source (according to the definition provided by the CRA) may undergo internal conformity assessment** even if they are “Important PDEs”.
- **Other PDEs** - PDEs that do not meet any of the other conformity can generally be declared by the manufacturer, following specific regulations. Anything that is not important or critical according to the CRA falls into this category unless otherwise regulated (e.g. medical devices).

**The CRA states that the EU will provide new acts to cover the specific classes and types of PDEs by mid-December 2025**, though initial examples are already available.

## **Compliance measures**

This section briefly lists the main compliance measures that manufacturers must undertake under the CRA. It is not complete or a full description, but gives an overview of most of the items most likely to affect manufacturers, and to which they should pay attention.

- **Conformance assessment**: this comes in two four types, depending on the class of the PDE ([Classes of PDEs](#)). Two of these involve internal assessment by the manufacturer, following the rules set out in the CRA, and the other two require external assessment by an approved assessment body.
- **Risk assessment: manufacturers must perform and document an initial risk assessment** across the entire supply chain for every PDE they will be making commercially available on the European market. This will be required for conformance assessment.
- **Technical documentation: manufacturers must compile technical documentation, which may include (for example) SBOMs information around supply chain, architecture, design, design processes and**

**deployment options. This will be required for conformance assessment** and some of it may be required to be made publicly available in certain circumstances.

- **Vulnerability status at release time: the CRA is clear that PDEs must “be made available on the market without known exploitable vulnerabilities”.**
- **Vulnerability management: there must be clear processes in place for vulnerability reporting and management, including releasing of updates and patches. An initial warning must be issued by manufacturers within 24 hours of their becoming aware of an actively exploited vulnerability, with further actions required at defined times.**
- **Incident reporting:** an initial warning **must be issued by manufacturers within 24 hours of their becoming aware of an incident** suspected of being caused by unlawful or malicious acts, with further actions required at defined times.
- **Free security updates: the manufacturer must make free security updates available to the public for 5 or more years in most cases.**

## Finding out more

For more information, we encourage you to:

- Visit the WG Repository: [Global Cyber Policy WG GitHub](#)

- Join Our Slack Channel: [#wg-globalcyberpolicy](#) on Slack
- Subscribe to Mailing Lists:
  - [Global Cyber Policy WG Mailing List](#)
  - [CRA Readiness+Awareness SIG Mailing List](#)
  - [CRA Tooling+Process+Formats SIG Mailing List](#)
  - [CRA Spec Standardization SIG Mailing List](#)