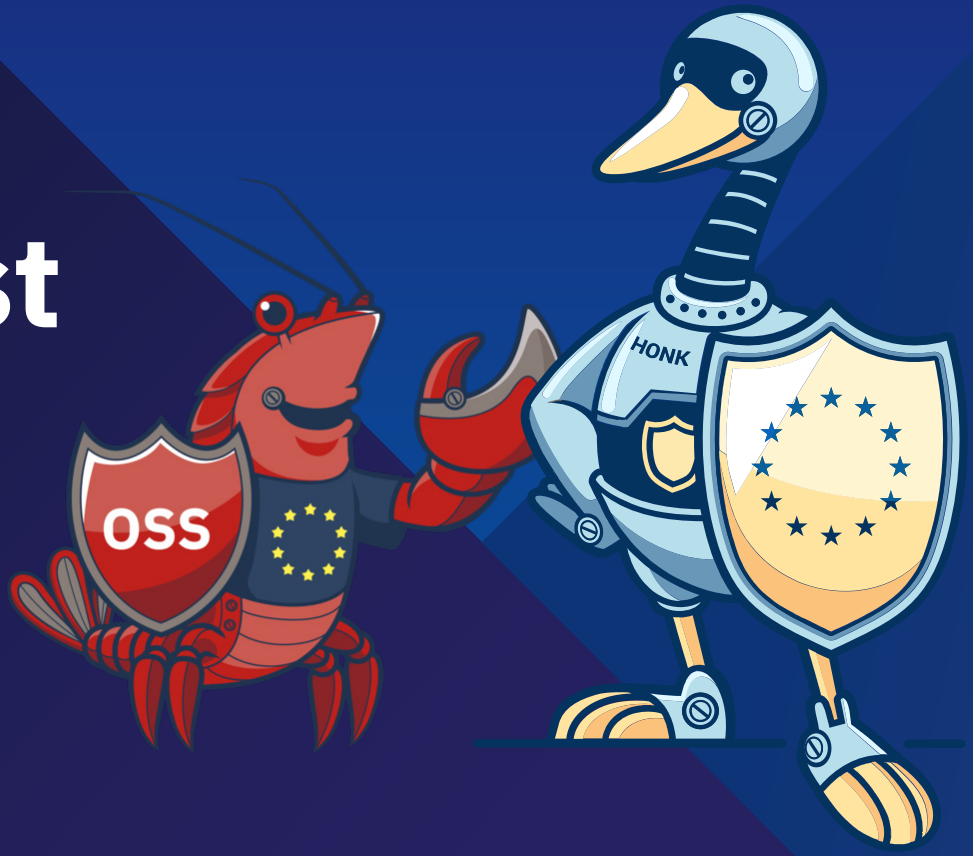
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Built to Last

Understanding the European Cyber Resilience Act (CRA)



Sal Kimmich
Policy Manager,
OpenUK

Version: 1.0 | July 2026

Executive Summary

The Cyber Resilience Act is law.

Regulation (EU) 2024/2847 entered into force on December 10, 2024. It applies directly across all EU member states without needing to be transposed into national law. It covers nearly every hardware and software product sold into the EU market. And for most organizations that make, import, distribute, or purchase digital products, it creates obligations that are already running.

This guide exists because the gap between what the CRA requires and what most organizations understand it to require is still significant.

Three deadlines define the compliance timeline. In June 2026, the framework for notifying conformity assessment bodies became operational. In September 2026, vulnerability reporting obligations take effect: manufacturers must notify actively exploited vulnerabilities to their national CSIRT and ENISA within 24 hours of becoming aware. That obligation applies to products already on the market, not just new releases. In December 2027, full enforcement begins and all products placed on the EU market must carry CE marking confirming conformity with the regulation's essential cybersecurity requirements.

This guide is structured around ten questions that practitioners, maintainers, legal teams, and buyers are actually asking. Each chapter is written to stand alone. You do not need to read it sequentially, though the chapters do build on each other.

Legal Disclaimer

What each chapter covers

Chapter 1: What Is the Cyber Resilience Act, and Why Does It Matter?
An orientation for every producer and buyer of digital products. What the CRA is, what it regulates, and why the assumption that it does not apply is already wrong for most organizations.

Chapter 2: How Do You Know If Your Product Is in Scope?
The tiered product classification system: default, important Class I and II, and critical. How to determine which conformity pathway applies to your product.

Chapter 3: Open Source Is Not Exempt. Here Is What the CRA Actually Says.
The commercial activity test, the open source software steward concept, and what even non-obligated maintainers should be doing now as commercial users begin asking new questions.

Chapter 4: Security by Design Is Now a Legal Requirement. What That Looks Like in Practice.
Annex I unpacked: the essential product requirements in Part I and the vulnerability handling obligations in Part II, translated into what engineering teams need to do and document.

Chapter 5: Vulnerability Reporting Under the CRA: A Practical Breakdown.
The three-step reporting process, the 24-hour clock, why September 2026 is the operative trigger for SBOM readiness, and how to build a CRA-compliant disclosure workflow.

Chapter 6: You Did Not Build It. You Are Still Responsible.
The obligations on importers and distributors. What due diligence looks like in practice, what supplier agreements need to say, and the specific position system integrators occupy.

Chapter 7: Conformity Assessment Under the CRA: What the Process Actually Involves.
The three conformity pathways, what notified bodies do and when they are required, what the technical file needs to contain, and where harmonized standards currently stand.

Chapter 8: The CRA Changes What Good Procurement Looks Like.
How buyers can use CE marking and conformity documentation as procurement signals, which vendor questions are now standard, and how to update supplier contracts appropriately.

Chapter 9: CRA Compliance for Small Teams: Where to Start When You Do Not Have a Legal Department.
The SME provisions, the minimum viable documentation set, and the free public resources that lower the compliance barrier for founders and small engineering teams.

Chapter 10: The CRA Does Not Stand Alone: Where It Sits in the EU Digital Sovereignty Framework.
How the CRA connects to NIS2, the AI Act, DORA, and the Data Act. The strategic case for treating CRA compliance as infrastructure rather than a one-time exercise.

Each chapter ends with primary source references. The regulatory citations used throughout this guide refer to the text of Regulation (EU) 2024/2847 as published in the Official Journal of the European Union on November 20, 2024, and to implementing and delegated acts adopted thereafter.

Contents

Executive Summary 2

What each chapter covers 3

Chapter 1: What Is the Cyber Resilience Act, and Why Does It Matter? 5

Chapter 2: How Do You Know If Your Product Is in Scope? 7

Chapter 3: Open Source Is Not Exempt. Here Is What the CRA Actually Says. 9

Chapter 4: Security by Design Is Now a Legal Requirement. What That Looks Like in Practice 11

Chapter 5: Vulnerability Reporting Under the CRA: A Practical Breakdown 13

Chapter 6: You Did Not Build It. You Are Still Responsible. 15

Chapter 7: Conformity Assessment Under the CRA: What the Process Actually Involves 17

Chapter 8: The CRA Changes What Good Procurement Looks Like 19

Chapter 10: The CRA Does Not Stand Alone: Where It Sits in the EU Digital Sovereignty Framework 23

Chapter 1: What Is the Cyber Resilience Act, and Why Does It Matter?

TL;DR: The CRA is EU law. It entered into force in December 2024. It covers nearly every hardware and software product sold into the EU market. If your organization makes, imports, distributes, or buys digital products, this applies to you.

A few years ago, if you asked a software vendor whether they expected to be subject to product safety law, most would have said no. Software was not a toaster. It did not have a CE mark. The rules for physical products did not translate.

That assumption is wrong now.

The Cyber Resilience Act, formally published as Regulation (EU) 2024/2847 on November 20, 2024, entered into force on December 10, 2024. It is not a directive. It does not need to be transposed into national law. It applies directly across all EU member states. And it covers a wider scope of products than most organizations have realized.

What the CRA actually regulates

The CRA applies to what it calls products with digital elements, or PDEs. The definition is broad: hardware, software, products containing them, and their backend services, if they are made available on the EU market. That includes consumer devices, industrial control systems, smart home products, operating systems, mobile apps, and much of the software that organizations sell or license into European markets.

There are exclusions. Medical devices, cars, aircraft, and other product categories with their own safety and security frameworks are carved out. But most general software and connected hardware is in scope.

The primary goal is to reduce the costs of data breaches and increase customer trust in products with a digital component. The secondary effect is a significant rebalancing of responsibility. Right now, when a product ships with known vulnerabilities, the cost of that decision is absorbed by the users and organizations who depend on it. The CRA shifts that cost back toward manufacturers, where the original decision was made.

Three dates you need to know

The CRA does not all kick in at once. There are three dates that matter:

June 11, 2026: The framework for notifying conformity assessment bodies becomes operational. This matters if your product falls into the important or critical categories.

September 11, 2026: Vulnerability reporting obligations start. From this date, if your product has an actively exploited vulnerability, you have 24 hours to report it to the relevant CSIRT and ENISA via the Single Reporting Platform. This applies to products already on the market, not just new releases.

December 11, 2027: Full enforcement. All essential cybersecurity requirements apply. Products must carry CE marking confirming conformity before they can be placed on the EU market.

Why the ‘it won’t affect me’ assumption is already failing

There is a common pattern in how organizations respond to new regulation. They wait for enforcement. They assume the scope is narrower than it is. They treat compliance as a late-stage legal problem rather than an early-stage engineering decision.

It’s worth understanding that the CRA does not require a “full” SBOM. Annex I, Part II(1) requires one that covers at least your top-level dependencies: your direct components, in a machine-readable format, kept current. That is the legal minimum, and it does not become enforceable until December 2027. You will not be penalised for failing to enumerate the seventh transitive dependency of a logging library.

The floor, however, should not be mistaken for the objective. Top-level visibility is precisely what fails you in a log4shell scenario, where the affected component sits several layers deep in something you did not author. The regulation permits you to stop at the surface; effective incident response does not.

This is why the operative deadline is September 2026, when the 24-hour reporting obligation takes effect. Once a vulnerability is disclosed, you have a single day to determine whether it affects your product, and this is often a question you cannot answer from a top-level inventory alone. It requires an accurate, current account of what you have actually shipped. In practice, that means building the more complete SBOM the CRA does not yet formally mandate, because it is the only way to meet the obligation it already demands.

Who is covered and in what role

The CRA distinguishes between manufacturers, importers, and distributors. Each role carries different obligations, and the distinctions matter. A manufacturer who designs and ships a product has the heaviest obligations. An importer who brings a product into the EU market from outside has its own due diligence requirements. A distributor who resells has obligations too.

Open source is not exempt by default, but non-commercial open source is treated differently. There is a new legal category called the open source software steward, designed for foundations and organizations that support open source development without acting as a manufacturer.

The rest of this eBook covers each of these roles in detail. But the starting position for any organization is the same: read the regulation, understand which role you occupy, and start the compliance work now.

The CRA is live. The clock is running. The question is not whether it applies to you. For most organizations, it does. The question is how far behind you are willing to fall before you take it seriously.

Resources: OpenSSF EU CRA page (openssf.org/public-policy/eu-cyber-resilience-act). Free Linux Foundation course: LFEL1001 Understanding the EU Cyber Resilience Act.

Chapter 2: How Do You Know If Your Product Is in Scope?

TL;DR: The CRA uses a tiered product classification system. Most products self-certify. Important and critical products face stricter requirements. The first step is understanding which tier you are in, because the conformity pathway depends on it.

The question I hear most from engineering and product teams is some version of: does this apply to us? The answer almost always requires two follow-up questions. What product are you making? And who are you selling it to in the EU market?

The CRA does not apply uniformly. It uses a risk-based tiering system, and which tier your product lands in determines the conformity pathway you have to follow.

The default category: most products

The default category covers the majority of digital products. Memory chips, mobile apps, smart speakers, computer games, consumer devices. If your product does not appear in Annex III or Annex IV of the regulation, or in the annexes to Implementing Regulation (EU) 2025/2392 which provides the technical descriptions for those categories, you are in the default category.

Default products can self-certify. The manufacturer carries out its own conformity assessment, generates the required technical documentation, and affixes the CE mark. That does not mean the process is light. It means a third party is not required to validate it. The obligations in Annex I still apply.

Important products: Class I and Class II

Annex III covers important products. These are divided into two classes based on the cybersecurity risk they present.

Class I examples include password managers, standalone browsers, VPNs, and network management systems. For these, a manufacturer can still self-certify if they apply harmonized standards. If harmonized standards are not used, a notified body assessment is required.

Class II examples include operating systems, firewalls, routers, microprocessors, and industrial control system software. For Class II products, a notified body is always required, regardless of which standards are applied.

The Commission published Implementing Act(EU) 2025/2392 in November 2025 to clarify the technical description of what constitutes important and critical product categories. That document is worth reading if you are doing the classification exercise. The key concept is core functionality: what does the product primarily do, and does that function map to the Annex III or Annex IV categories?

Critical products

Annex IV covers critical products including secure elements, smart cards, smart meter gateways, hardware security modules, and are examples. Critical products require mandatory notified body assessment in every case. There is no self-certification pathway.

What ‘placing on the market’ means

The CRA applies when a product is placed on the market or made available on the EU market. This is a specific legal concept. It means the first time a product is made available for distribution or use in the EU market in the course of commercial activity, whether for payment or free of charge.

This matters for SaaS and software-as-a-service models. SaaS that functions as remote data processing for a product with digital elements is in scope. Standalone SaaS that does not provide remote data processing for a PDE is out of scope under Recital 12, falling instead under the NIS2 directive rather than the CRA.

The Commission’s **FAQ** and **draft guidance** have started to address this, but it remains an area where organizations should get specific legal advice rather than rely on general summaries.

Non-EU companies are not exempt

The CRA applies regardless of where the manufacturer is based. A US company selling software into the EU is a manufacturer under the CRA. A Japanese hardware company selling into the EU market is in scope. The territorial reach mirrors other EU digital regulation. If you want EU market access, you accept the obligations.

This has practical implications for non-EU companies with EU customers. You need to determine your product tier, carry out the appropriate conformity assessment, and have the required documentation ready before products ship.

The classification exercise is not optional

The right place to start is a product inventory. For each product or product line, run the classification test. Does it have a digital element? Is it made available in the EU market in the course of commercial activity? Does its core functionality map to Annex III or Annex IV?

If you have not done this exercise, you do not know your conformity pathway. And if you do not know your conformity pathway, you cannot know how much time you have or what resources to allocate.

Start with the product. The compliance pathway follows from there.

Resources: EC Implementing Regulation (EU) 2025/2392 on product categories. EC CRA conformity assessment page: digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment.

Chapter 3: Open Source Is Not Exempt. Here Is What the CRA Actually Says.

TL;DR: Individual open source contributors who are not monetizing their code do not have direct CRA obligations. But the commercial use of open source triggers obligations for manufacturers who integrate it. Foundations and support organizations may qualify as stewards, which carries its own lighter-touch obligations.

When the CRA was first proposed, the open source community had a strong and justified reaction. The early drafts created real ambiguity about whether maintainers would bear legal obligations for code they published freely. That ambiguity sparked significant engagement from foundations, working groups, and individual contributors.

The final text is better. It is not perfect. But it is important to understand what it actually says rather than what the early drafts implied.

The basic rule for individual contributors

If you contribute to someone else's open source project, or publish your own code without monetizing it, the CRA does not apply to you. That is stated clearly in the regulation. Non-commercial open source is outside the scope. The **OpenSSF CRA Brief Guide for OSS Developers** and the **OpenSSF CRA Guide for Maintainers** both address this directly.

What counts as commercial activity? Charging a fee for the product. Charging for technical support at rates that go beyond recovering actual costs — though the mere fact of offering support services does not itself constitute commercial activity, as clarified in section 3.2.3 of the Commission guidance. Intending to monetize through a platform. Collecting personal data for reasons beyond security, compatibility, or interoperability. Accepting donations that exceed costs.

If none of those apply, you are outside the scope of the CRA as a manufacturer.

What happens when open source is used commercially

Here is where the picture gets more complicated. If a manufacturer integrates your open source component into a product they sell on the EU market, the manufacturer bears the compliance obligation for that component. The CRA makes manufacturers responsible for the full product, including third-party and open source dependencies.

This has a practical downstream effect even for maintainers who are not directly subject to the CRA. Manufacturers are required to carry out due diligence on the components they use and to report vulnerabilities to upstream maintainers. Projects that are well-documented, have clear vulnerability disclosure processes, and produce SBOMs will be preferred. Projects that lack these things will face pressure from commercial users to produce them.

OpenSSF's Christopher Robinson made this point clearly: even developers not directly subject to the CRA should understand it, because commercial users will start asking for documentation, patches, and artifacts that they previously did not require.

The steward category

The CRA introduces a new legal concept: the open source software steward. A steward is a legal entity that systematically provides sustained support for the development of open source software intended for commercial activities, without filling the role of manufacturer.

Foundations like The Linux Foundation, Apache Software Foundation, and Eclipse Foundation are the obvious examples. An organization can be a steward for one project and a manufacturer for another.

Stewards have lighter obligations than manufacturers, but they are not zero. The obligations under Article 24 include: providing a cybersecurity policy, cooperating with market surveillance authorities and providing certain information when requested, reporting known actively exploited vulnerabilities, notifying about severe incidents, informing affected users, and providing mitigation.

There is no requirement for an open source project to have a steward. A project can operate without one. If a foundation or organization chooses to act as a steward, they accept those obligations.

What maintainers should do now

Even if you are clearly outside the CRA's direct scope, there are practical steps worth taking now.

Document your project's security practices. The OpenSSF Open Source Project Security Baseline provides a 41-practice checklist organized across three maturity levels. Most of what the CRA requires of manufacturers overlaps with good security hygiene regardless of regulatory context.

Set up or formalize a vulnerability disclosure process. A clear security contact and a documented cybersecurity policy and a vulnerability reporting process will be asked for by commercial users operating under the CRA. If you do not have one, you will spend time answering ad hoc requests from every organization that integrates your code.

Understand your monetization status honestly. The commercial activity test is not about intent in isolation. If you are accepting more in donations than you spend, if you are building a business model around the project, the CRA applies. The OpenSSF guide is clear on this: as soon as you try to monetize the software as a product, things change.

The CRA represents a significant shift in how the EU treats software security. The open source community engaged with that shift and influenced the final text. Understanding what the final text actually says is the next step.

Resources: OpenSSF CRA Brief Guide for OSS Developers (best.openssf.org/CRA-Brief-Guide-for-OSS-Developers.html). Linux Foundation CRA Stewards Playbook (policy.openssf.org/CRA/stewards-playbook.html). OpenSSF Open Source Project Security Baseline (baseline.openssf.org).

Chapter 4: Security by Design Is Now a Legal Requirement. What That Looks Like in Practice.

TL;DR: Annex I of the CRA sets the essential security requirements for products with digital elements. These are legal obligations, not design principles. Understanding what they require in practice is the difference between a compliant product and a product that fails its first market surveillance check.

Security by design has been a principle in the security community for years. The CRA makes it a legal requirement across the EU market. That is a meaningful shift. Principles can be interpreted loosely. Legal requirements have to be demonstrated.

Annex I is where the engineering work starts. It sets out two groups of requirements. Part I covers the properties of the product itself. Part II covers vulnerability handling. Together, they define what a compliant product looks like from a security perspective.

What Part I of Annex I requires

Part I lays down the baseline properties a product must have when it is placed on the market. The CRA requires that products are designed, developed, and produced to ensure an appropriate level of cybersecurity based on the risks.

That risk-based framing matters. The obligations are proportionate. A smart thermostat and an industrial control system are not subject to identical controls. But the obligation to carry out a risk assessment and implement appropriate measures applies to both.

The key requirements from Part I:

Products must ship without known exploitable vulnerabilities. This is a hard requirement. Shipping a product that contains a known CVE that is exploitable is a non-compliance on day one.

Products must ship with a secure default configuration. Users should not need to reconfigure a product to make it secure. Security must be the out-of-the-box state.

Access control must be implemented appropriately. Authentication, identity management, and access control mechanisms must match the risk profile of the product.

Confidentiality and integrity of stored, processed, and transmitted data must be protected.

The attack surface must be minimized. Unused interfaces, ports, and services should not be present in the default configuration.

Products must be designed to handle errors and avoid crashes that create exploitable conditions.

What Part II of Annex I requires

Part II covers vulnerability handling over the product's support period. This is where a lot of organizations underestimate the scope of the obligation.

Manufacturers must identify and document vulnerabilities and components, including by producing a Software Bill of Materials in a commonly used machine-readable format covering at least top-level dependencies. Technically, this SBOM obligation does not become enforceable until December 2027. But as discussed in Blog 1, you cannot meet the September 2026 vulnerability reporting obligation without SBOM-level visibility into your product's components.

Manufacturers must implement coordinated vulnerability disclosure processes, including a clear contact point for reporting vulnerabilities. They must fix vulnerabilities and make patches available. They must declare a support period for the product, which must be at least five years unless the product's expected lifecycle is shorter.

The support period end date must be communicated clearly at point of purchase. This is a transparency obligation. Users need to know when a product will stop receiving security updates.

What this means for engineering teams

The CRA is product-centric, not organization-centric. Your existing Information Security Management System covers internal governance. The CRA requires product-level evidence of compliance. These are related but not the same thing.

Practically, this means secure Software Development Lifecycle implementation needs to produce artifacts that can be reviewed by market surveillance authorities. Threat models need to be documented. Risk assessments need to be defensible.

The harmonized standards being developed under Mandate M/606 are the operative reference for CRA conformity. The ENISA standards mapping document provides useful background for understanding the Annex I requirements, but existing standards such as ISO 27001 or IEC 62443 should not be treated as a basis for CRA conformity assessment. Manufacturers who build their compliance programs around those standards now risk duplication of effort, since it is unclear whether market surveillance authorities will treat them as relevant evidence. Track the M/606 standards as they develop and engage a notified body where harmonized standards are not yet available.

The CRA does not prescribe implementation methods. It sets outcome requirements. How you get there is a design decision. That is deliberate, and it is appropriate given the range of products in scope. But it means the justification for your choices has to be documented and defensible.

Start with the risk assessment. Everything else in Annex I flows from there.

Resources: ENISA CRA Requirements Standards Mapping. EC CRA Annex I text: eur-lex.europa.eu/eli/reg/2024/2847/oj. OpenSSF Concise Guide for Developing More Secure Software: best.openssf.org.

Chapter 5: Vulnerability Reporting Under the CRA: A Practical Breakdown

TL;DR: From September 11, 2026, manufacturers and stewards must report actively exploited vulnerabilities to ENISA within 24 hours and submit a full notification within 72 hours. This applies to products already on the market, not just new releases. If your vulnerability management process cannot meet that timeline, you are not ready.

September 11, 2026 is the date most product security teams should be working backward from right now. That is when the CRA's vulnerability and incident reporting obligations become enforceable. It is earlier than the main enforcement date of December 2027, and it catches more products than many organizations expect.

Article 69(3) of the CRA is explicit: the reporting obligations in Article 14 apply to all products with digital elements that have been made available on the market, including products placed on the market before December 2027. If you shipped a product in 2020 and it is still in use, and it develops an actively exploited vulnerability, you must report it from September 2026.

The three reporting steps

Article 14 of the CRA sets out a three-step notification process. All notifications go through the CRA Single Reporting Platform (SRP) operated by ENISA, which will be operational by September 2026. ENISA has published an FAQ on the SRP for organizations preparing now.

Step one: early warning. Within 24 hours of becoming aware of an actively exploited vulnerability, the manufacturer must submit an early warning to the relevant CSIRT (the national Computer Security Incident Response Team for the member state where the manufacturer has its main EU establishment) and simultaneously to ENISA.

Step two: full notification. Within 72 hours of becoming aware, a full vulnerability notification must follow, unless the relevant information was already included in the early warning.

Step three: final report. No later than 14 days after a corrective or mitigating measure is available for actively exploited vulnerabilities. For severe incidents, within one month of becoming aware.

What 'actively exploited' means in practice

The 24-hour clock starts when the manufacturer becomes aware. Not when the vulnerability is publicly disclosed. Not when a CVE is assigned. When the manufacturer knows. This is an internal knowledge threshold, and it creates an incentive for manufacturers to maintain real-time visibility into their components.

This is why the SBOM is not just a compliance artifact. Without component-level visibility, you cannot know whether a newly disclosed CVE affects your product until someone manually investigates. Manual investigation takes days. You have 24 hours.

Organizations that have SBOM-based vulnerability monitoring set up before September 2026 will be able to run automated checks against vulnerability databases as new CVEs are published. Organizations that do not have this will be constantly at risk of exceeding the reporting window.

How this interacts with existing CVD processes

The CRA reporting obligation runs alongside, not instead of, existing coordinated vulnerability disclosure (CVD) processes. CVE assignment, NVD publication, and vendor advisories continue to operate as before. The CRA adds a mandatory regulatory reporting layer on top.

The notification goes to the CSIRT of the member state where the manufacturer has its main EU establishment. That CSIRT then distributes the notification to other member state CSIRTs where the product is known to be available, and ENISA receives the notification simultaneously.

There are exceptions. Under Delegated Regulation (EU) 2026/881, the receiving CSIRT may delay dissemination to other CSIRTs on justified cybersecurity grounds: for example, where a patch is expected within 72 hours, where the notification detail is sensitive enough that sharing it could itself enable exploitation, or where there are serious concerns about a particular CSIRT's ability to protect the information. Any delay must be strictly limited to the time necessary, and ENISA must be informed immediately of the decision to delay and the reasons for it. If the product is only available in the member state of the receiving CSIRT, no dissemination to other CSIRTs is required at all.

For non-EU manufacturers, the main establishment is determined by where key cybersecurity decisions for the product are made within the Union. Non-EU manufacturers without any EU establishment may need to designate an EU representative.

The SME fine exemption is not what it sounds like

The CRA includes a provision that manufacturers qualifying as microenterprises or small enterprises may not be fined for failures to meet the 24-hour reporting deadline. This has been misread in some coverage as a general exemption for small companies.

It is not. The obligation to report still applies. The exemption is limited to the penalty for missing the 24-hour window, not for failing to report at all. Small companies still have to build the capability to report. They just have some protection from fines if the first report comes in slightly late.

Building a CRA-compliant disclosure process

A compliant internal process needs several components working together: SBOM generation and maintenance for each product, automated vulnerability monitoring against public databases (EUVD, NVD, OSV, CISA KEV catalog, GitHub advisories), a clear escalation path that can trigger the 24-hour window from first internal awareness, and a tested mechanism for submitting notifications through ENISA's SRP.

Organizations that already have PSIRT processes for CVD have a foundation to build from. The CRA adds regulatory reporting requirements on top of that foundation. If you do not have a PSIRT process, the CRA is the reason to build one now, not in 2027.

Resources: ENISA Single Reporting Platform FAQ (enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp). CRA Article 14 full text (european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_14.html). EC reporting obligations page (digital-strategy.ec.europa.eu/en/policies/cra-reporting).

Chapter 6: You Did Not Build It. You Are Still Responsible.

TL;DR: The CRA puts obligations on importers and distributors, not just manufacturers. If you bring a product with a digital element into the EU market, you carry compliance responsibility. Due diligence is not optional, and 'the manufacturer told us it was compliant' is not a defense.

There is a common assumption in distribution and reseller channels that compliance responsibility sits with whoever made the product. The CRA directly challenges that assumption.

Importers and distributors have their own obligations under the regulation. The scope of those obligations is different from what manufacturers face, but they are not light, and they apply to every organization that makes products with digital elements available in the EU market.

The importer's role

An importer, under the CRA, is any natural or legal person established in the EU who places a product with digital elements from a third country on the EU market.

Before placing a product on the market, importers must verify that the manufacturer has carried out the appropriate conformity assessment. They must check that the required technical documentation exists. They must confirm that the product bears CE marking, includes the EU Declaration of Conformity, and carries the required instructions and safety information.

Importers must also verify that the manufacturer has a vulnerability handling process in place. You cannot import a product, verify its CE mark, and then ignore the question of whether the manufacturer will actually patch vulnerabilities during the product's support period. The CRA requires you to check.

If an importer has reason to believe a product is not in conformity with the CRA, they must not place it on the market until conformity is achieved. They must also inform the manufacturer and, where appropriate, market surveillance authorities.

The distributor's role

A distributor is any person in the supply chain, other than the manufacturer or importer, who makes a product with digital elements available on the EU market.

Distributors must check that the product bears the CE mark and includes the required instructions and information before making it available. They must not make a product available if they have reason to believe it does not comply with the CRA's essential requirements.

If a distributor becomes aware of a vulnerability in a product they have distributed, they must notify the manufacturer. If they have reason to believe the product presents a cybersecurity risk, they must inform the manufacturer and market surveillance authorities. They must cooperate with market surveillance in eliminating risks.

What this means for supplier agreements

The practical implication is that supplier agreements need to change. The contract between an importer or distributor and a manufacturer needs to address CRA conformity explicitly.

At minimum, supplier agreements should require: confirmation of the appropriate conformity assessment for each product, access to the technical documentation and Declaration of Conformity, a commitment to maintain vulnerability handling

processes for the declared support period, and a notification obligation if the manufacturer becomes aware of a vulnerability that affects products supplied to you.

Some organizations will want to go further and require audit rights, SLAs on vulnerability notification timelines, and contractual liability clauses linked to CRA non-conformity. The level of contractual protection should match the level of risk you are accepting.

System integrators occupy a specific position

System integrators who combine components from multiple manufacturers into a system that is placed on the EU market need to think carefully about their role. Depending on how the integration works and how the final product is sold, the integrator may be acting as a manufacturer under the CRA.

If you take components, integrate them into a solution, and sell that solution as a product, you are likely a manufacturer. The CRA requires you to carry out the conformity assessment for the integrated system, not just rely on the conformity of the individual components.

This is an area where legal advice specific to your product and business model is essential. The general principle is that the entity that places the product on the market takes responsibility for it.

The bottom line

The CRA rebalances responsibility along the supply chain. That was deliberate. Products with digital elements have historically been allowed to enter the EU market with insufficient security documentation and no clear vulnerability handling commitments. The CRA closes that gap by assigning obligations to every economic operator in the chain.

If you import or distribute digital products, start your supplier due diligence now. The December 2027 deadline is closer than it looks when you factor in supplier renegotiation timelines.

Resources: EC CRA summary (digital-strategy.ec.europa.eu/en/policies/cra-summary). CRA Article 20 (distributor obligations) and Article 19 (importer obligations) at european-cyber-resilience-act.com.

Chapter 7: Conformity Assessment Under the CRA: What the Process Actually Involves

TL;DR: Most products can self-certify under the CRA. Important products in Class I may also self-certify if harmonized standards are applied. Class II important products and all critical products require a notified body. Harmonized standards are still being developed. That creates an immediate decision point about which conformity pathway to use.

CE marking for software is one of the most significant structural changes the CRA introduces. For most of the history of EU product law, software did not carry CE marks. The CRA changes that. And with CE marking comes a conformity assessment process.

Understanding the pathway for your product category is one of the first practical decisions a compliance team needs to make.

The three conformity pathways

Default products: Most hardware and software falls into the default category. These products use Module A (internal conformity assessment) where the manufacturer assesses their own product against the Annex I requirements, generates the technical documentation, produces the EU Declaration of Conformity, and affixes the CE mark. No third party is required.

Important products, Class I: These include password managers, standalone browsers, VPNs, and network management systems. Class I products can use Module A if they apply harmonized European standards. If harmonized standards are not used, they must go through a notified body using either Module B+C (EU type examination followed by conformity to type) or Module H (full quality assurance system assessment). Because harmonized standards for the CRA are still being developed by European standardisation bodies, many Class I manufacturers will need to go through a notified body for the initial certification cycle.

Important products: Class II and critical products: Class II includes operating systems, firewalls, routers, and microprocessors. Critical products under Annex IV include secure elements, smart cards, and smart meter gateways. Both always require a notified body, regardless of which standards are applied. The notified body assessment follows either Module B+C or Module H. Module B+C involves product-level type examination and suits stable product lines. Module H is based on a full quality assurance system audit and offers more flexibility where a manufacturer has multiple products or frequent updates, since extending scope to new products is more streamlined than repeating a full type examination.

What a notified body does

Conformity assessment bodies are, in general terms, private companies that test and certify products. Under the CRA, they must be assessed, designated, notified, and monitored by the member state where they are established before they can operate as CRA notified bodies.

The notified body framework under the CRA does not become operational until June 11, 2026. Member states are required to

strive to ensure there is a sufficient number of notified bodies by December 2026. This is a tight timeline. Organizations whose products require notified body assessment should be identifying potential notified bodies now, before demand outstrips supply.

The CRA also has a provision that products certified under an EU cybersecurity certification scheme may not require notified body participation, with the exact conditions to be specified by the Commission. EUCC (the European Cybersecurity Certification Scheme for Common Criteria) is the most relevant existing scheme for high-assurance products.

The technical documentation requirement

Whether you use internal assessment or a notified body, you need a technical file. The CRA specifies the contents in Annex VII. It includes a product description and the intended use, a list of harmonized or other standards applied, the cybersecurity risk assessment, a description of the design and production process and monitoring procedures, the EU Declaration of Conformity, and records of vulnerability handling.

This documentation must be maintained and kept available to market surveillance authorities for at least ten years after the product is placed on the market, or for the duration of the support period if that is longer.

Harmonized standards and where they stand

Harmonized standards are the technical specifications that, when applied, create a presumption of conformity with the CRA requirements. They are being developed by ETSI, CEN and CENELEC. As of mid-2026, first drafts are beginning to emerge, but full harmonized standard coverage for the CRA's Annex I requirements is not yet available.

This is a practical problem for manufacturers on the Class I pathway. Without harmonized standards to reference, they must engage a notified body for Module B+C or Module H assessment. Existing standards such as ISO 27001, IEC 62443, or NIST frameworks are not a substitute: no formal gap analysis has been done between those standards and the CRA-specific standards being developed under Mandate M/606, so they cannot be used to claim a presumption of conformity.

The harmonized standards being developed under Mandate M/606 are the operative reference for CRA conformity. The ENISA standards mapping document provides useful background for understanding the Annex I requirements, but existing standards such as ISO 27001 or IEC 62443 are not a basis for conformity assessment under the CRA and should not be treated as one.

Manufacturers who build their compliance programs around those standards now risk duplication of effort, since it is unclear whether market surveillance authorities will treat them as relevant evidence. The practical path is to track the M/606 standards as they develop and engage a notified body where the harmonized standards are not yet available.

Resources: EC CRA conformity assessment page (digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment). BSI CRA guidance (bsi.bund.de). ENISA standards mapping. EU NANDO database for notified bodies (once CRA entries are available).

Chapter 8: The CRA Changes What Good Procurement Looks Like

TL;DR: The CRA shifts security liability upstream toward producers. Buyers benefit from stronger baseline guarantees on products sold into the EU. But those guarantees only work if procurement processes are updated to verify conformity and ask the right questions of vendors.

One of the underappreciated effects of the CRA is on the buyer side. Most of the regulation's obligations fall on producers, importers, and distributors. But the entire regulatory architecture is built around improving security outcomes for the people and organizations that use digital products. Buyers can use that architecture as a procurement tool.

The CRA does not create direct legal obligations for enterprise buyers purchasing commercial software and hardware. But it does change what responsible procurement looks like.

CE marking as a procurement signal

From December 2027, products with digital elements sold into the EU market must carry CE marking confirming conformity with the CRA's essential requirements. That mark, backed by a Declaration of Conformity and technical documentation, is a signal that the manufacturer has carried out the required risk assessment, addressed the Annex I requirements, and committed to maintaining vulnerability handling for the declared support period.

In practice, CE marking alone is not sufficient as a procurement criterion. The conformity assessment for most products is self-declared. A Declaration of Conformity is the manufacturer's statement that the product meets the requirements, not an independent audit result. For high-assurance environments, especially those covered by NIS2 or DORA, buyers should look beyond the CE mark to the underlying technical documentation and the conformity pathway used.

Questions to ask vendors

Effective procurement under the CRA means asking vendors questions they were not routinely expected to answer before December 2024. Useful questions include:

What product category does this fall under, default, Class I, or Class II? If Class I or II, what conformity pathway was followed and which notified body was used if applicable?

What is the declared support period, and when does it end? This must be communicated at point of purchase under the CRA. If a vendor cannot answer this clearly, that is itself a compliance signal.

What is your coordinated vulnerability disclosure process? Where is your security contact published? What is your average time from vulnerability awareness to patch availability?

Do you produce SBOMs for this product? In what format? Are they available to customers?

How do you meet the September 2026 vulnerability reporting obligation? Do you have the monitoring infrastructure to detect actively exploited vulnerabilities within 24 hours of their occurrence?

These are not exotic questions. They are the standard of care the CRA is attempting to establish across the market. Organizations that make these questions routine in their vendor evaluation process will be better positioned than those that rely on questionnaire-based self-attestation.

Supplier contract updates

Procurement contracts need to reflect the CRA's obligations. At minimum, contracts should require conformity with the CRA for products sold into the EU market, a commitment to maintain vulnerability handling for the support period, notification to the buyer when an actively exploited vulnerability is discovered in a product they have purchased, and access to technical documentation on request.

More mature procurement frameworks will add SLAs on vulnerability notification timelines, audit rights on vulnerability handling processes, and contractual liability clauses linked to CRA non-conformity that results in a security incident.

One point worth being explicit about: open source projects are not suppliers in the contractual sense. A manufacturer who integrates an open source component bears the CRA compliance obligation for that component themselves. The due diligence obligation runs to the manufacturer, not to the upstream project.

Attempting to push contractual CRA obligations onto open source maintainers misreads the regulation and reflects a misunderstanding that surfaced early in standardization discussions. The CRA is clear that the manufacturer is responsible for what they ship, regardless of where the components originated.

Public sector considerations

Public sector organizations often have additional obligations under NIS2 as essential or important entities. The intersection of NIS2 supply chain security requirements and CRA product conformity creates a situation where public sector buyers have both regulatory drivers to update procurement processes.

The CRA's transparency requirements, the published declaration of conformity, the declared support period, the documented vulnerability handling process, create a baseline of verifiable information that public sector procurement can and should incorporate into tender evaluation criteria.

The CRA is designed to make the EU digital market safer. The full benefit is only realized if buyers use the information the regulation requires producers to publish. Start using it now.

Resources: EC CRA summary (digital-strategy.ec.europa.eu/en/policies/cra-summary). ENISA guidance on CRA requirements. DORA and NIS2 supply chain security provisions for intersection guidance.

Chapter 9: CRA Compliance for Small Teams: Where to Start When You Do Not Have a Legal Department

TL;DR: The CRA has specific provisions for SMEs, but they do not remove the obligations. They reduce some barriers. Smaller teams need to prioritize ruthlessly: classify your product, understand your conformity pathway, and build the minimum viable documentation set before December 2027.

I am not going to tell you compliance is easy. For a team of three people trying to ship a product, the CRA represents a genuine additional burden. The regulation acknowledges this. Article 33 of the CRA specifically addresses support measures for micro-enterprises, SMEs, and startups.

But acknowledging the burden is different from removing it. The obligations apply. The difference is that smaller companies have some structural advantages in how they navigate them, and there are resources specifically designed to lower the barrier.

What the SME provisions actually do

Microenterprises and small enterprises that miss the 24-hour vulnerability reporting deadline cannot be fined for that specific failure. The obligation to report still applies. The exemption is narrow: it covers the penalty for the 24-hour window only, not for the reporting obligation itself.

The notified body fee structure is required to take the size of the organization into account. If your product needs third-party conformity assessment, notified bodies are required to consider the size of the undertaking, including microenterprises, when setting fees.

Member states are expected to provide regulatory sandboxes and testing environments to help SMEs comply. The SECURE project (Strengthening EU SMEs Cyber Resilience) offers financial support and guidance specifically for SMEs navigating CRA compliance.

The Commission published **technical FAQs** in December 2025 and **draft guidance** in March 2026, with a particular focus on microenterprises and SMEs. The draft guidance covers scope questions, remote data processing, FOSS treatment, support periods, and the interplay with other EU legislation. It is not yet final and is not legally binding, but it is the most current statement of the Commission's interpretive position and worth reading now.

The first priority: classify your product

Everything starts with product classification. Is your product in the default category, Class I, or Class II? This single determination defines your conformity pathway.

For most startups and indie developers, the product will be in the default category. Default products can self-certify. That means a manageable process if you approach it methodically.

If your product uses a network interface, handles authentication, or relates to cybersecurity functions, check Annex III carefully. Password managers, for example, are Class I. A startup building a password manager needs a notified body if they are not applying harmonized standards.

The minimum viable documentation set

For a default product, the minimum documentation required for CRA conformity is:

A cybersecurity risk assessment for the product. This does not need to be extensive, but it needs to be documented, defensible, and proportionate to the actual risk the product presents.

Evidence of how the Annex I Part I requirements are met. This covers the product properties: secure by default, no known exploitable vulnerabilities at release, minimal attack surface, appropriate access control, data protection.

A due diligence report covering the third-party and open source components integrated into the product. The CRA requires manufacturers to exercise due diligence over the components they ship. That obligation needs to be documented.

A Software Bill of Materials, or at least a component inventory that can be used to track known vulnerabilities. The formal SBOM requirement is Annex I Part II and is enforceable from December 2027. But component visibility is required for the September 2026 reporting obligation.

A vulnerability disclosure policy and security contact. This needs to be publicly available. Publish it on your website.

A Declaration of Conformity. This is the formal statement that the product meets the CRA's requirements. The format is specified in Annex V.

A declared support period for the product, communicated at point of purchase.

Free resources that reduce the barrier

The Linux Foundation offers a free express course: **LFEL1001, Understanding the EU Cyber Resilience Act (CRA)**. It covers the basics and comes with a digital badge. Complete it before making any compliance decisions.

The OpenSSF **Open Source Project Security Baseline** provides a 41-practice checklist that covers the security behaviors the CRA is trying to mandate. If your project meets the baseline, you are most of the way to a defensible Annex I compliance narrative.

The **OpenSSF CRA Brief Guide for OSS Developers** is specifically written for individual developers and small teams. It explains the scope clearly and without jargon.

The CRA is not designed to exclude small teams from the EU market. It is designed to raise the baseline of security across all products. For small teams building genuinely secure products, the documentation burden is real but achievable. Start with the risk assessment, work through the Annex I checklist, and publish a vulnerability disclosure policy. That is the foundation. Build from there.

Resources: Free LF course LFEL1001. OpenSSF Security Baseline (baseline.openssf.org). SECURE project for SMEs (secure4sme.eu). EC draft SME guidance (watch digital-strategy.ec.europa.eu for publication). EC Article 33 support measures.

Chapter 10: The CRA Does Not Stand Alone: Where It Sits in the EU Digital Sovereignty Framework

TL;DR: The CRA is one piece of a broader EU regulatory architecture. It connects to NIS2, the AI Act, the Data Act, and DORA in ways that create both compliance overlaps and strategic opportunities. Understanding those connections changes how you think about CRA compliance investment.

Most organizations are treating the CRA as a standalone compliance exercise. That is understandable. The regulation is substantial and the timelines are tight. But treating it in isolation means you are likely duplicating work across multiple regulatory frameworks and missing the opportunity to build compliance capabilities that serve more than one regulatory obligation.

The CRA sits within a coherent, if not always perfectly coordinated, EU digital regulatory stack. Understanding where it connects to other frameworks is how you make the compliance investment efficient.

CRA and NIS2

NIS2 (Directive (EU) 2022/2555) focuses on organizational resilience for essential and important entities. It requires risk management, incident reporting, supply chain security, and business continuity measures at the organizational level. The CRA focuses on product security. They are product-centric and organization-centric versions of related obligations.

The connection is supply chain security. NIS2 requires essential and important entities to assess the security of their supply chains, including the cybersecurity practices of their suppliers and the security properties of the products and services they procure. The CRA creates a framework of verifiable product security information: conformity assessments, Declarations of Conformity, SBOMs, vulnerability handling commitments.

That gives NIS2-obligated entities concrete, standardized artifacts to use in that assessment. Organizations subject to NIS2 supply chain security requirements can use CRA conformity as a structured, verifiable component of their supplier evaluation process, rather than relying on questionnaire-based self-attestation alone.

For organizations subject to both NIS2 as an entity and CRA as a manufacturer, the governance, risk assessment, and incident response processes can be designed to serve both frameworks rather than run as parallel tracks.

CRA and the AI Act

Article 12 of the CRA creates an explicit connection to the EU AI Act. If a product with a digital element is also a high-risk AI system under the AI Act, compliance with the CRA's product requirements and vulnerability handling processes in Annex I can be used to demonstrate compliance with the AI Act's cybersecurity requirements under Article 15.

This is a genuine efficiency. Organizations building AI products that qualify as high-risk AI systems under the AI Act and that are also covered by the CRA can design their security and

vulnerability management processes once and use them for both regulatory purposes.

The intersection also creates complexity. Products that are important or critical under the CRA have their own conformity assessment requirements that take precedence over AI Act internal control provisions for cybersecurity aspects. The two frameworks are connected but not fully merged.

CRA and DORA

DORA (the Digital Operational Resilience Act) applies to financial entities and their ICT service providers. It is organization-centric, like NIS2, but with specific provisions around ICT third-party risk management.

DORA's ICT third-party risk management requirements create a due diligence obligation toward suppliers of digital products and services. CRA conformity is a relevant input to that due diligence. Financial entities subject to DORA and their technology suppliers navigating CRA have aligned interests in building interoperable compliance documentation.

CRA and the Data Act

The Data Act (Regulation (EU) 2023/2854) applies to connected products and related services. A product with a digital element may simultaneously qualify as a connected product under the Data Act. Where both regulations apply, manufacturers face overlapping obligations around data access, documentation, and user transparency.

The Commission has acknowledged this overlap. CRA compliance programs that account for Data Act obligations from the start will be more efficient than those that treat them as separate workstreams.

The strategic read

Taken together, the CRA, NIS2, the AI Act, DORA, and the Data Act are part of a broader attempt to establish baseline security and transparency standards across the EU digital market. Each addresses a different failure mode: insecure products, insecure organizations, unsafe AI systems, operationally fragile financial infrastructure, and opaque data practices. This is not an exhaustive list of relevant EU digital legislation, but these are the frameworks most likely to create overlapping obligations for organizations navigating CRA compliance.

The enforcement timeline for the CRA is December 2027. NIS2 has been in force since October 2024. The AI Act is applying in phases from 2024 through 2027. DORA has applied to financial entities from January 2025.

Organizations that are building compliance programs now have an opportunity to design governance, risk, and documentation infrastructure that serves multiple frameworks. Organizations that wait until each deadline approaches will build separate, fragmented programs that cost more and provide less.

The CRA is not the end of the EU digital regulatory build-out. It is one installment. The organizations that approach it as a one-time compliance exercise will repeat this work. The ones that build durable capability now will not.

Get Involved

The regulatory landscape for open source software shifts quickly. Stay informed by visiting the **OpenSSF policy page** for resources and updates. To help shape our strategic approach, join the **Global Cyber Policy working group**. We invite you to contribute your expertise to this critical mission.

About the Author

Sal Kimmich is a developer advocate and security engineer working at the intersection of open source governance, software supply chain security, and privacy-enhancing technologies. They serve as a contributor to the Open Source Security Foundation's Education SIG, BEAR WG, and co-chair of the CHAOSS data science WG. Sal helps build inclusive pathways as an international open source community leader, known for mentoring first-time contributors and shaping policy around secure development practices across Europe, the UK, and North America. By day, you'll find Sal filling in the gaps of the latest threat models for agentic AI systems; in their free time, they mentor the next generation of exceptional engineering talent and help them find their voice in open source security.

Resources: EC CRA policy page (digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act). NIS2 Directive (EU) 2022/2555. EU AI Act Regulation (EU) 2024/1689. Digital Operational Resilience Act (EU) 2022/2554. Data Act (EU) 2023/2854.

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

openssf.org