prime security

What is the EU Cyber Resilience Act?

The EU Cyber Resilience Act (CRA) is **binding law** that sets mandatory cybersecurity requirements for digital products sold in the EU.

It **applies before products reach the market** and requires **security to be designed in by default**, not added later.

The CRA is about proving that security decisions were made intentionally, documented, and justified — **before code is written.**

Key dates to know

CRA entered into force (became law)	Mandatory vulnerability and incident reporting obligations apply	Full CRA requirements become enforceable	Procurement, customer reviews will move 12–18 months ahead of enforcement
December 10 **2024**	September 11 **2026**	December 11 **2027**	

Am I affected?

The CRA applies to **any company that places products with digital elements on the EU market,** regardless of where the company is headquartered. You are **directly in scope** if you:

- Distribute software into the EU (desktop, mobile, embedded, on-prem, SDKs, agents, extensions)
- Embed software in hardware or connected devices
- White-label or bundle digital products sold in the EU

Pure SaaS vendors,

where no software is delivered to the customer, are generally **out of scope as products**. However, SaaS offerings **are in scope** if they include any distributed component, such as: a downloadable client or agent, a mobile application, an on-prem or self-hosted component, a browser extension, etc.

What are the key requirements?

- **Identify and mitigate foreseeable security risks before release**
- Maintain **secure development practices across the product lifecycle**
- **Handle vulnerabilities systematically**, including detection, remediation, and customer communication
- **Reassess risk as products evolve**, so new features or integrations don't introduce unmanaged exposure
- **Provide evidence of due care**, showing how and why security decisions were made - including risk acceptance

The CRA is **risk-based and proportional**, but one thing is universal: **documented, repeatable security decision-making is no longer optional**.

What's the "stick"?

- **Fines** (up to the higher of €15M or 2.5% of global annual turnover)
- **Market access restrictions** (products can be blocked from the EU market)
- Mandatory remediation, recalls, or product withdrawals

The CRA goes beyond ISO 27001, NIS2, and DORA. Those frameworks focus on how your organization manages security; the CRA focuses on the **security of the products you build and sell.** It requires products to be **secure by design**, resilient to attack, and continuously maintained throughout their lifecycle.

What should you know about "Secure by Design"?

Under the CRA, the question is: **"Can you prove security decisions were made early - and consistently?"**

Security risks are identified before implementation, when decisions are still cheap to change	Risks are evaluated in the context of **architecture, data flows, integrations, and intended use**	**Security decisions are intentional, documented, and repeatable** — not ad hoc	Risk is **continuously reassessed** as products and features evolve

This represents a fundamental shift. Security can no longer rely on:

Reviewing only a small sample of work	One-off threat modeling workshops	Post-release fixes as the primary control

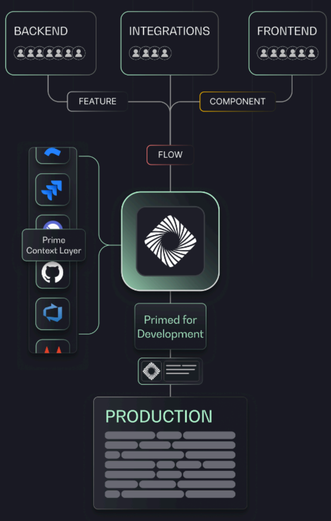
prime security

How Prime Helps

Why Prime Exists

The CRA doesn't care how many security tools you have.
It cares whether you can prove control over security decisions - before code ships.

Prime exists to make that possible. As an Agentic Security Architect, Prime enables Product Security teams to identify, reason about, and document design-stage risk across 100% of planned development work, at the scale and consistency the CRA demands.



◆ Continuous design-stage risk management

Prime continuously analyzes **planned work before code exists** - PRDs, Jira tickets, epics, architecture changes, integrations, and new initiatives.

This allows teams to:

- ✓ Maintain visibility across **100% of planned changes**
- ✓ Identify **foreseeable design-stage risk early**
- ✓ Understand **which components and initiatives introduce the highest risk**
- ✓ **Re-evaluate risk automatically** as designs evolve
- ✓ Create an **auditable living evidence trail** for every review that aligns directly with CRA expectations

Prime gives you auditable risk evidance

What risk was identified and **why**	How it was prioritized	What mitigation was recommended	Where risk was accepted, with rationale	Whether the mitigation was implemented

◆ Scalable, automated risk reviews

Prime provides **automated, repeatable security and privacy design reviews** for every feature or component - without slowing engineering.

This replaces:	The result:
⊘ Ad hoc threat modeling	✓ Identifies design-stage security and privacy risks
⊘ Inconsistent guidance across teams	✓ Produces clear, actionable mitigation guidance
⊘ Security becoming a bottleneck as velocity increases	✓ Assesses risk in the context of architecture, data flows, integrations, and intended use
	✓ Documents security decisions in a consistent, repeatable format

◆ Validation and prioritization - closing the loop

Prime continuously validates that:

- Mitigations were implemented as designed
- Accepted risks are intentional and documented
- High-risk components receive appropriate attention

By aggregating risk across planned work, Prime helps teams:

- Identify risk hotspots across products and teams
- Focus effort on the highest-impact security decisions
- Avoid spending time on low-risk noise

◆ What this means for CRA readiness

With Prime, organizations can:

- Operationalize **secure by design** across the entire product surface area
- Scale Product Security without scaling headcount
- Enable developers to move faster **without losing control**
- **Prove due care on demand** and show defensible proof of secure-by-design decision-making
- Provide clear **answers for procurement, auditors, and regulators**
- **Continuously provide audit and regulatory** documentation

Prime helps you to increase review velocity and
prove control over design stage product risk

Want to learn more?

Talk to an Expert at
primesec.ai/meet-prime-security

Proudly backed by:

foundation capital · FLYBRIDGE · SCALE VENTURE PARTNERS

Contact us:
support@primesec.ai