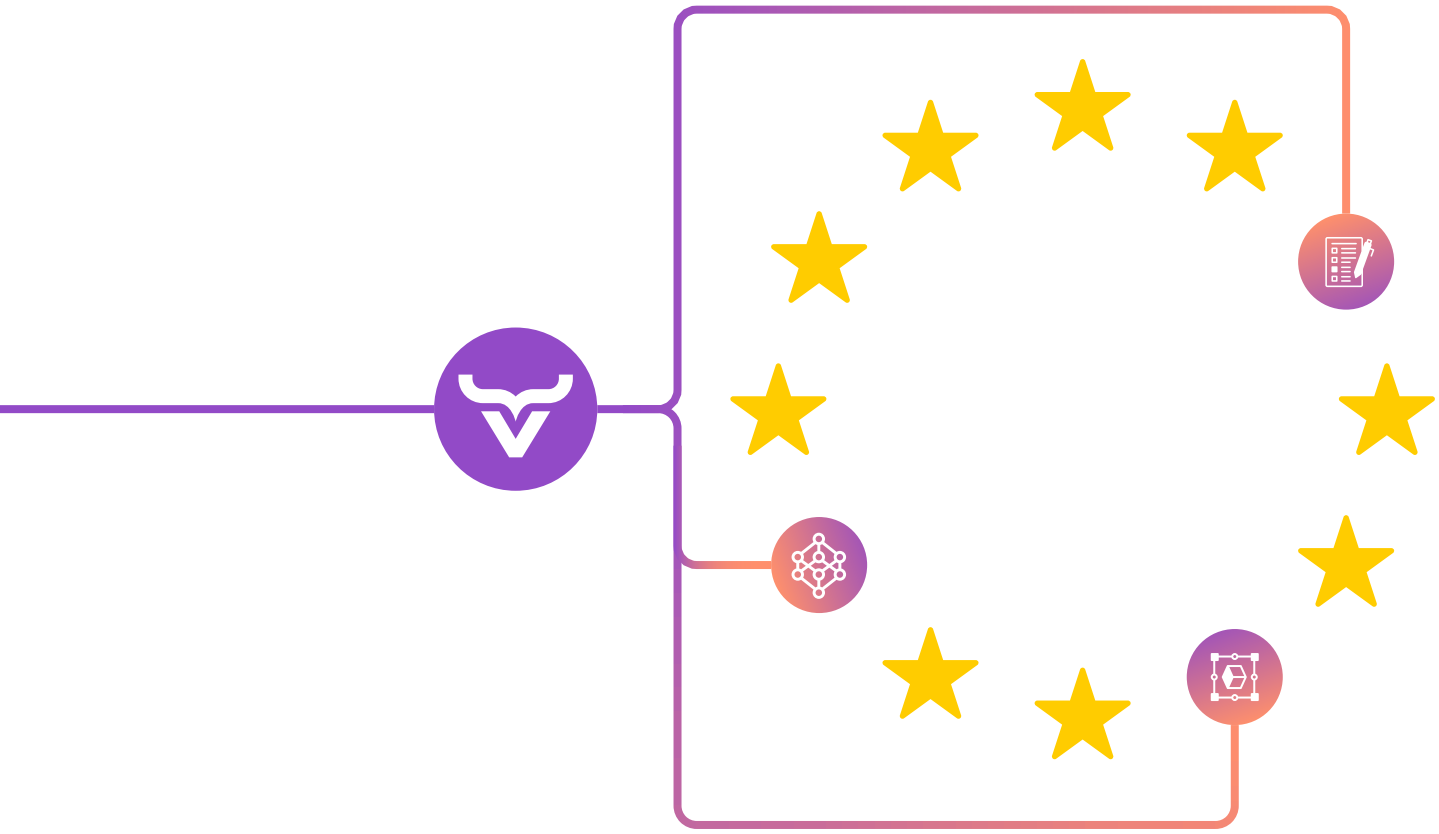

Leveraging OX Security for EU Cyber Resilience Act (CRA) Compliance

A Practical Guide for AppSec and Product Security Leaders

Presented By OX

July 2025

Executive Summary

The European Union's Cyber Resilience Act (CRA) isn't just another piece of paper; it's a major shift in global cybersecurity governance. This binding framework demands "secure by design" principles and relentless security measures across the entire lifecycle of products with digital elements (PDEs). Its overarching objective is to shield end-users and forge a more resilient digital world by holding manufacturers, importers, and distributors squarely accountable for the cybersecurity posture of their products. This regulatory mandate is specifically designed to counteract the escalating threats posed by cyberattacks and to address the historical problem of pushing insecure products to market.

In this evolving landscape, OX Security's Unified AppSec platform presents a strategic solution for organizations navigating the complexities of CRA compliance. By unifying disparate AppSec tools, providing comprehensive end-to-end visibility through its proprietary Pipeline Bill of Materials (PBOM), and leveraging extensive automation, OX Security directly addresses the fundamental requirements of the CRA. This includes fostering secure development practices, robust vulnerability management, comprehensive reporting, and continuous monitoring throughout the product lifecycle. The platform's ability to precisely prioritize exploitable vulnerabilities, and its seamless integration into existing development workflows, significantly streamlines the journey toward regulatory adherence.

This report will detail how OX Security's capabilities align with and facilitate compliance with the CRA. It will illustrate how the OX platform transforms compliance from a potentially reactive burden into a proactive, competitive advantage by systematically enhancing product security, accelerating vulnerability remediation, and cultivating greater trust among customers and regulatory bodies.

Understanding the Cyber Resilience Act (CRA)

The CRA is the EU's newest move to supercharge cybersecurity across every connected device and digital service. The Act's core mission? To ensure that "products with digital elements" (PDEs) — meaning, everything from customers' smart fridges to their enterprise software — are meticulously designed, developed, and maintained with hardened security from day one, through their entire operational lifecycle. This isn't a suggestion by the government; it's a mandate that every digital product designer and developer must embrace by embedding secure-by-design principles into the core product, then committing to delivering continuous updates to protect against evolving cyber threats.

The Act isn't just about protecting customers, the end-user; it takes direct aim at the projected **$10.5 trillion cost of global cybercrime in 2025**. It's also a cultural wake-up call for organizations and how they really prioritize cybersecurity. To be viable on the European market, digital products must contain fewer vulnerabilities, and builders/manufacturers must relentlessly manage security throughout the product's lifespan.

The CRA's scope is massive, encompassing virtually all PDEs whose intended use involves any form of direct or indirect logical or physical data connection to a device or network. This broad definition includes a wide array of products, such as Internet of Things (IoT) devices, mobile and desktop applications, embedded systems, operating systems, and industrial control software (ICS).

Crucially, the Act extends its regulatory reach to manufacturers (the people and organizations responsible for producing and delivering PDEs), providers (those supplying components or software, whether open-source or proprietary), importers, and distributors. This applies to all entities, regardless of geographic location, whose products are available on the EU market.

> **The emphasis on embedding security from the outset signals a cultural transformation within organizations, extending beyond technical implementation.**

A central tenet of the CRA is the imperative for products to be "secure by design and default." This principle dictates that cybersecurity must be intrinsically integrated at every phase of the product lifecycle — from initial concept and design through development, deployment, and ongoing maintenance. It necessitates:

- Minimizing potential attack surfaces
- Hardening devices against compromise
- Safeguarding data through robust encryption
- Preventing unauthorized access
- Ensuring continuous operational functionality even under distributed denial-of-service (DDoS) attacks
- Providing comprehensive security data through continuous monitoring and logging

The emphasis on embedding security from the outset signals a cultural transformation within organizations, extending beyond technical implementation. The requirement for cross-functional planning underscores this organizational requirement. This implies a fundamental change in organizations' approach to security, transitioning from viewing security as an afterthought to establishing it as a proactive, ingrained core design principle and a shared responsibility across the entire enterprise.

Organizations that proactively embrace secure-by-design and perceive it as an opportunity are positioned to meet regulatory mandates and also establish a significant competitive advantage. By demonstrating a commitment to security through highly secure products, companies can differentiate themselves in a market increasingly attuned to cyber risks

This strategic approach transforms compliance from a cost center into a powerful driver of value and a cornerstone of brand reputation.

Core CRA Compliance Obligations: A Multi-faceted Approach

When approaching a mandate as large as CRA, a fundamental question is always: **How can my organization begin its alignment with CRA?**

To start, organizations must devise a process in which security is integrated throughout the entire product lifecycle. Manufacturers must address cybersecurity considerations at every stage: design, development, deployment, and ongoing maintenance.

This includes processes and programs that:

- Implement secure default configurations to inherently reduce vulnerabilities from the outset; and
- Provide regular updates and fixes to sustain security even after product deployment

Specific measures that manufacturers must undertake to protect systems include controls to:

- Harden devices
- Prevent unauthorized access and use
- Ensure data protection through robust cryptographic methods

Next, organizations must establish strong processes to find, track, and respond to security issues, including those in third-party components. This requires organizations to fix problems quickly, issue clear updates to users, and run regular tests to catch new risks early.

Furthermore, manufacturers must set clear, transparent rules for reporting and handling security issues. They must notify authorities like such as Computer Security Incident Response Teams (CSIRTs) and the European Union Agency for Cybersecurity (ENISA)within 24 hours of discovering an actively exploited vulnerability or major incident. They also need to provide users enough information to identify affected products, understand the risk, and follow steps to fix it. A “security.txt” file must be posted online, showing how to report issues (including anonymously) and where to find security advisories.

Third, the CRA requires organizations to create and maintain a Software Bill of Materials (SBOM). This entails the creation and ongoing maintenance of an SBOM, which serves as a detailed and accessible inventory of all components, particularly third-party and open-source code, integrated within a product. This level of transparency is vital for organizations to comprehensively understand product composition, identify potential vulnerabilities, and effectively manage risks across the software supply chain. What’s more, SBOMs must be included in the technical documentation and are key to information sharing.

Fourth, manufacturers must continuously monitor their systems and be ready to respond to emerging threats. Organizations need to establish clear processes for applying patches and updates to keep pace with changing risks. If a serious security incident or actively exploited vulnerability is found — especially one caused by a malicious act — they must alert national CSIRTs and ENISA within 24 hours and follow up with a report in two weeks. They must also inform users and provide timely fixes or guidance to reduce harm.

Finally, businesses must complete risk assessments and maintain clear documentation to prove CRA compliance. This includes details on product design, delivery, vulnerability management, risk handling, SBOMs, and user manuals. Products are ranked by risk — Default, Important (Class I/II), and Critical — which determines whether a self-assessment or third-party review is needed. All approved products must display the CE mark to show they meet CRA cybersecurity standards.

Implications of Non-Compliance and Key Deadlines

The implications of non-compliance with the CRA are a serious business risk. Failing to meet the CRA's mandates carries severe implications: fines up to €15 million or 2.5% of the business's global annual turnover — whichever is higher — depending on the severity of the violation. But it's not just about the financial ramifications; non-compliance can harm the company's reputation, risking loss of customers, partners, and/or global market share.

The CRA officially entered into force on December 10, 2024. However, the implementation of its requirements is phased:

- **Incident and vulnerability reporting obligations** become enforceable by September 11, 2026. This provides manufacturers with a 21-month grace period from the Act's official publication to adapt their reporting mechanisms and ensure readiness.
- **Full compliance with all CRA obligations,** including SBOM mandates and the requirement for CE marking, is mandatory by December 11, 2027. Businesses are given a 36-month grace period from the CRA's official publication to fully adapt their products and processes.

OX Security and CRA: A Unified AppSec Platform

Enter OX Security: the Unified AppSec platform that's engineered to pull an organization's fragmented AppSec tools into one singular, cohesive system. The foundational vision centers on empowering organizations with a solution that doesn't just put out today's fires but proactively anticipates tomorrow's infernos. A primary objective? Ditching those manual AppSec tasks that leave security and development teams "drowning in manual AppSec tasks".

A cornerstone of OX Security's approach is its **continuous scanning and contextual prioritization** capabilities. The platform performs continuous scanning across the entire software development lifecycle, diligently analyzing code, dependencies, containers, and cloud environments from the initial design phase through runtime operations. A significant differentiator is its sophisticated ability to prioritize identified vulnerabilities based on their actual exploitability, reachability within the system, and their potential business impact. This intelligent prioritization enables OX Security to pinpoint and highlight "only the top 5% of exploitable vulnerabilities". This precise focus dramatically reduces alert fatigue, allowing security teams to allocate their resources and attention to the most critical and impactful threats, thereby optimizing their remediation efforts.

How OX Security Facilitates CRA Compliance

OX Security is a unified platform that helps organizations cut through AppSec complexity and focus on what's actually important. Instead of juggling multiple tools and drowning in low-priority alerts, security and development teams get a clear view of what needs fixing—and why.

OX continuously scans across the software development lifecycle, covering code, dependencies, containers, and cloud environments. But it doesn't just flag issues—it helps teams understand which ones are exploitable, reachable, and relevant to their business. That means less noise, fewer false alarms, and faster response where it matters most.

This approach is especially valuable for organizations preparing for the EU Cyber Resilience Act (CRA). OX supports key CRA requirements by helping AppSec and DevOps teams:

- Maintain continuous visibility into software components and vulnerabilities throughout the entire product lifecycle
- Practice shift-left security, allowing them to build securely from the start
- Automatically generate and update SBOMs for visibility and auditing purposes
- Verify artifact integrity across the build and deployment process
- Rigorously prioritize and manage vulnerabilities based on reachability, exploitability, and business impact in the organization's specific environment, with their specific build
- Streamline remediation and tracking for reduced risk and attack surface management
- Automated workflows for incident reporting and mitigation
- Provide traceable, auditable records of remediation and risk management activities

Table 1: CRA Compliance Requirements and Corresponding OX Security Capabilities

Key CRA Requirement	Specific CRA Mandate/Action	OX Security Capability	How OX Security Addresses It
Integrate Security Throughout Product Lifecycle	Secure by Design/Default; address security at every stage (design, dev, deploy, maintenance); secure default configs; regular updates and fixes.	Continuous end-to-end scanning; shift-left security; developer-centric UI with guided fix paths.	Integrates security checks from code inception to release; enables early identification and remediation of issues in development workflows; reduces risk of introducing vulnerabilities.
Vulnerability Management and Disclosure	Identify and document vulnerabilities (incl. 3rd-party); swift response, automatic updates, clear advisories; regular testing and auditing; transparent disclosure policies; notify authorities (CSIRT, ENISA) of exploited vulns/incidents within 24 hrs.	Automated identification and prioritization; streamlined remediation and tracking; AI-assisted remediation; no-code workflows.	Automatically scans, prioritizes (top 5% exploitable) based on severity/exploitability/impact; provides tools to track remediation progress; accelerates fixes from weeks to days; supports data needed for disclosure.
SBOM Generation	Create and maintain detailed SBOMs (incl. 3rd-party/open-source); Share SBOMs with stakeholders/regulators.	Pipeline Bill of Materials (PBOM).	Automatically generates and maintains dynamic, real-time inventory of all software components; provides comprehensive, up-to-date visibility across SDLC for transparency and risk management.
Continuous Monitoring and Incident Response	Continuously monitor infrastructure for threats; dynamic patch/update process; comprehensive incident response procedures; notify authorities of incidents within 24 hrs; Inform users about incidents and mitigation.	Real-time visibility and threat detection; automated workflows for incident reporting and mitigation.	Provides continuous scanning across code, containers, cloud for emerging threats; automates ticketing and notifications for internal response; streamlines data gathering for rapid regulatory reporting.
Conformity Assessments and Documentation	Conduct risk assessments; Prepare technical documentation (design, vul. mgmt, risk assessment, SBOM, manuals); classify products by risk; Adhere to scrutiny levels (self-assessment or 3rd-party).	Compliance reporting; automated reporting and documentation; dynamic software lineage list.	Generates reports demonstrating compliance (vul. mgmt, SBOM, incident response); provides evidence for audits; centralizes security data for comprehensive technical documentation.

Strategic Benefits of OX for Cyber Resilience

PROACTIVE ADAPTABILITY TO EVOLVING REGULATIONS

Regulatory requirements like the CRA are expanding, and staying compliant means having the ability to adapt — without rebuilding processes every time something changes.

OX supports these efforts by giving organizations a clear, traceable view of their software components, build processes, and security posture. Features like automated SBOM and PBOM generation, artifact integrity checks, and policy enforcement help teams prepare for current CRA requirements, and adjust when new ones arrive.

Instead of treating compliance as a one-off task, OX incorporates it into day-to-day operations, which reduces last-minute work and ensures teams remain audit-ready.

REDUCE SECURITY DEBT AND ACCELERATING REMEDIATION

Finding every possible vulnerability isn't helpful if teams can't fix them. OX focuses on exploitable and reachable vulnerabilities so teams can respond to the one that will have a substantive impact on the organization.

The OX Platform filters out noise and connects the remaining issues to clear fix paths, helping teams reduce security debt without burning time on low-risk work. Built-in workflows and integrations allow for faster resolution, often without involving multiple teams or manual coordination.

For organizations facing CRA timelines and reporting requirements, using OX to achieve these goals:

- Shortens remediation cycles;
- Reduces exposure; and
- Builds evidence of risk management without extra overhead.

ENHANCE DEVELOPER PRODUCTIVITY AND COLLABORATION

Security requirements often add friction to development. OX is designed to limit that friction by fitting into the tools and processes developers already use.

The platform integrates with systems like GitHub, GitLab, and Jenkins, and provides issue detail and remediation context inside developer workflows — no extra portals, no handoffs. Fixes are supported by AI-generated suggestions that are specific to the codebase, not generic templates.

Instead of treating compliance as a one-off task, OX incorporates it into day-to-day operations, which reduces last-minute work and ensures teams remain audit-ready.

This helps development and AppSec teams work together more efficiently. Developers can address valid issues quickly, and AppSec teams gain visibility without needing to micromanage or chase updates.

Summary

The EU's Cyber Resilience Act introduces new expectations for how organizations develop, secure, and maintain digital products. Meeting these requirements requires full visibility into software, strong control over vulnerabilities, and clear documentation throughout the development lifecycle.

OX helps teams meet (and then exceed) CRA expectations with a single platform that connects code to cloud. Organizations gain:

- Full visibility across the software lifecycle
- Real-time insight into supply chain components via its Pipeline Bill of Materials (PBOM)
- Clear prioritization of vulnerabilities based on actual risk
- Automated workflows for remediation, reporting, and incident response

Rather than relying on fragmented tools and manual processes, OX supports a consistent, repeatable approach to security that's aligned with how modern software is built and delivered.

Recommendations for Organizations Considering OX Security

For businesses ready to tackle CRA compliance, here are some actionable recommendations to start up-leveling your AppSec program and processes:

Conduct a detailed gap analysis

Thoroughly map current application security practices against all CRA requirements using the detailed obligations outlined in this report. This step is crucial for pinpointing exactly where OX Security's capabilities can fill compliance gaps, especially for secure-by-design principles, continuous monitoring, and comprehensive SBOM generation.

Prioritize integration and shift-left

OX seamlessly integrates with existing version control systems, CI/CD pipelines, and developer tools (e.g., GitHub, Jenkins, Azure DevOps). This integration capability maximizes the benefits of a "shift-left" approach, ensuring security checks are an intrinsic part of the development lifecycle from the earliest stages of software development.

Embrace automation for scale and speed

Actively implement OX Security's no-code workflows and AI-assisted remediation suggestions to automate vulnerability management and incident response processes. This automation is critical for meeting the CRA's stringent reporting timelines (like that 24-hour incident notification!) and for efficiently managing and reducing security debt at scale within a continuous delivery environment.

Use PBOM for enhanced supply chain transparency

Fully leverage OX's PBOM for dynamic, real-time visibility into the entire software supply chain, including third-party and open-source components. Doing so aids CRA compliance by providing the mandated transparency. PBOM also affords OX customers a strategic advantage in proactively managing supply chain risks and demonstrating comprehensive control to all stakeholders.

Align security with business strategy

View CRA compliance not merely as a regulatory obligation but as a significant opportunity to enhance product security, build customer trust, and gain a competitive advantage. By investing in a comprehensive AppSec solution like OX, organizations can transform their cybersecurity posture into a strategic differentiator, fostering long-term resilience and market leadership.

About OX

OX Security revolutionizes application security by eliminating the distraction of generic prioritization and enabling teams to focus on the 5% of risks that truly matter. Traditional ASPM tools overwhelm security and development teams with commoditized alerts, wasting resources and slowing progress.

With OX's proprietary technology, organizations gain precise risk prioritization based on exploitability, reachability, and business impact — ensuring vulnerabilities are addressed before they reach runtime.

By integrating security seamlessly into the development lifecycle, OX replaces fragmented, siloed tools with a unified approach that empowers AppSec teams to act faster, reduce risk efficiently, and support developers without unnecessary friction.

OX.SECURITY