BLACK DUCK®

CHECKLIST

EU CRA VULNERABILITY REPORTING CHECKLIST: SEPT ’26 OBLIGATIONS

The European Union (EU) Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for software and hardware products sold in the EU, covering security by design, vulnerability handling, and ongoing maintenance obligations across the total product life cycle.

Beginning September 11, 2026, the CRA enters into an enforcement phase requiring manufacturers, importers, and distributors, to notify ENISA and designated national CSIRTs of actively exploited vulnerabilities and severe security incidents.

Is your organization ready to meet CRA vulnerability reporting requirements? Our helpful checklist can help you prepare.

IN-SCOPE PRODUCTS

The CRA defines a product classification system that includes a default category for all software, as well as increasingly stringent classifications based on primary product functions. The CRA excludes products with alternative cybersecurity obligations such as medical devices. Penalties for nonconformance include fines that are a percentage of global revenue (of all nonconforming products) and/or removal of the products from the European market. Products covered by the CRA include those that meet the following criteria:

- ☐ Product is a "product with digital elements" (software, firmware, embedded software, software required for a connected product to function)
- ☐ Product is commercially distributed in the EU (free open source software without commercial activity is generally excluded)
- ☐ Product is not already subject to more stringent, industry-specific regulations
- ☐ Legacy products sold on the EU market are in scope; the requirements are not limited to new releases

MANDATORY REPORTING TIMELINES

- ☐ Early warning must be filed within 24 hours of becoming aware of an actively exploited vulnerability or severe security incident (note that this 24-hour timeline isn't for triage or resolutions; it is intended only as an early warning system)
- ☐ Triage report must be filed within 72 hours after triage of the vulnerability concludes and must contain a resolution path (e.g., a plan to fix or determination that the vulnerability doesn't impact the product)
- ☐ Final report covering lessons learned and process improvements must be submitted within 14 days after remediation is available
- ☐ Reporting capabilities must be operational and tested before September 2026

SBOM REQUIREMENTS

- ☐ SBOMs must be generated for every shipped product version
- ☐ SBOMs must be in a standardized format (SPDX or CycloneDX)
- ☐ SBOMs must be stored for potential review by market surveillance authorities
- ☐ There is no requirement to share SBOMs with any third parties other than market surveillance authorities

CONTINUOUS VULNERABILITY MONITORING

- ☐ Manufacturers, distributors, and importers must implement a continuous vulnerability monitoring process designed to identify changes in supply chain risk as communicated via the European Vulnerability Database (EUVD) or other data sources as defined by the European Commission
- ☐ Monitoring tools must prioritize potentially exploitable vulnerabilities
- ☐ Monitoring must align with the role of the product within its supply chain (e.g., if company A produces something consumed by company B, company A must ensure that it doesn't ship that product with potentially exploitable vulnerabilities)

REPORTING INFRASTRUCTURE

- ☐ Integration with the CRA single reporting platform must be planned or tested
- ☐ Internal policies and playbooks must describe vulnerability and incident reporting over the total product life cycle, including support periods
- ☐ All cybersecurity decision-making, including tooling selection, must be documented (including, for example, success criteria for tooling and its alignment with CRA obligations, who processed a vulnerability and how they arrived at its disposition, and who communicates externally)

SECURE BY DESIGN EVIDENCE

- ☐ Product risk assessment must be conducted and documented
- ☐ Vulnerability handling process must be documented and repeatable
- ☐ Logs and records must be retained to prove compliance actions

Must-Have by September 11, 2026

- Vulnerability monitoring and processes aligned with Article 14
- SBOM-driven visibility
- Reporting workflows and timelines
- Disclosure and update processes

Due in 2027

- CE marking
- Full conformity assessment
- Harmonized standard compliance

HOW BLACK DUCK CAN HELP

Black Duck provides tools designed to meet the stringent requirements of the CRA.

- Black Duck® SCA identifies third-party risk and clearly indicates when a vulnerability in the EUVD is exploitable, allowing companies to meet their 24-hour reporting requirements.
- Coverity® Static Analysis identifies first-party risks that could become third-party risks if not properly addressed prior to shipping a product with digital elements to a customer within a supply chain.
- Defensics® Fuzzing identifies first- and third-party risk associated with cyber-physical devices, assemblies and subassemblies, and spare parts.

By helping teams identify open source and third-party components, track vulnerabilities, and establish repeatable processes for managing software risk, Black Duck supports the foundational practices needed to meet CRA vulnerability management and reporting obligations.

To learn how Black Duck can support your organization's CRA readiness efforts, contact us to start the conversation.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.