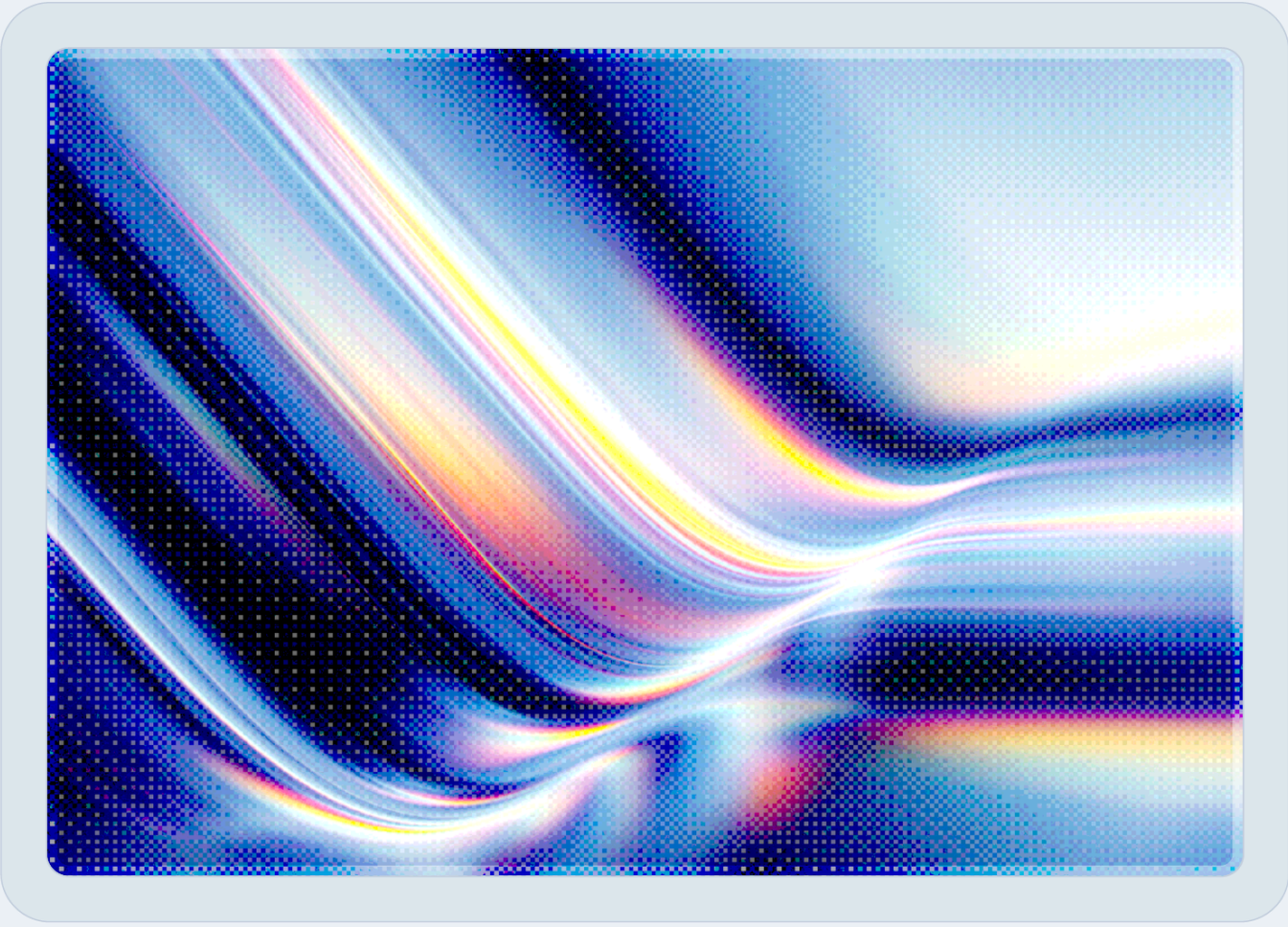
CSAI Foundation | Cloud Security Alliance

CRA Reporting Clock Starts: ENISA's Single Reporting Platform Live

2026-09-14

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

The CRA's first legally binding operational obligation for manufacturers took effect on September 11, 2026, when ENISA's Single Reporting Platform (SRP) went live and the reporting duty under Articles 13 and 14 became enforceable [1][2]. Manufacturers of products with digital elements sold into the EU market must now report actively exploited vulnerabilities and severe incidents to a national CSIRT coordinator and ENISA through a single online portal, on a clock that starts at 24 hours and does not pause for weekends or holidays [3][4]. The obligation applies prospectively to legacy products already on the EU market, not only new releases, a scope choice that CSA's prior analysis suggests many manufacturers are not yet operationally prepared for [5]. Non-compliance with the reporting duty (Articles 13 and 14) sits in the CRA's top penalty tier, exposing manufacturers to fines of up to €15 million or 2.5% of global annual turnover, whichever is higher [6]. Given the survey evidence on incident-response maturity discussed later in this note [5], organizations without an intake, triage, and escalation process for this obligation should treat September 11 as a deadline already missed rather than one still approaching.

Background

The Cyber Resilience Act, formally Regulation (EU) 2024/2847, entered into force in December 2024 and imposes cybersecurity requirements on manufacturers, importers, and distributors of "products with digital elements" sold in the EU — a category broad enough to capture everything from consumer IoT devices to industrial control systems and standalone software [4][6]. The regulation was designed to phase in over roughly three years, giving industry time to build the processes, documentation, and tooling the law requires. Conformity assessment bodies began registering under the CRA in June 2026, and the law's full essential cybersecurity requirements — secure-by-design engineering, vulnerability handling processes, CE marking, and technical documentation — do not become mandatory until December 11, 2027 [5][7].

Reporting obligations, however, were carved out for earlier enforcement, and that earlier date arrived on September 11, 2026. From that date, manufacturers must notify authorities when they become aware of a vulnerability in their product that is being actively exploited, or of a severe incident affecting the security of a product with digital elements [3][4]. ENISA defines active exploitation narrowly: there must be reliable evidence that a malicious actor has exploited the vulnerability in a system without the system

owner's permission, not merely that the vulnerability is theoretically exploitable or has a public proof-of-concept [4]. Open-source software stewards — foundations, maintainers' organizations, and similar entities involved in developing components used in covered products — fall under the same reporting duty starting December 11, 2027, a fifteen-month grace period relative to the manufacturer deadline [1] [2].

To operationalize the reporting duty, ENISA was mandated to build and run a common electronic reporting mechanism, and it delivered the Single Reporting Platform, which opened for use on the same day the obligation became mandatory [1][2]. Rather than requiring manufacturers to separately notify each EU member state where an affected product is sold, the SRP lets a manufacturer file once; the CSIRT designated as coordinator for that submission then disseminates the notification to other relevant member-state CSIRTs and to ENISA simultaneously, with dissemination delayed only under exceptional circumstances where early distribution would itself create security risk [2][3]. ENISA's Executive Director framed the platform's purpose directly around this consolidation: vulnerabilities in digital products are routinely exploited to disrupt critical services, and a coordinated single point of intake is intended to strengthen the EU's collective response without multiplying the reporting burden per member state [1].

Security Analysis

The SRP's most consequential design feature for security teams is not the platform itself but the timeline it enforces. A manufacturer that becomes aware of an actively exploited vulnerability or a severe incident must submit an early warning within 24 hours, a fuller structured notification within 72 hours of that early warning, and a final report no later than 14 days after a corrective measure becomes available for a vulnerability, or within one month of the 72-hour notification for a severe incident [3][4]. Legal commentary on the rule describes what this means operationally in specific terms: the clock starts when an organization reaches a "reasonable degree of certainty" that a reportable event exists, and it runs continuously, including over weekends and public holidays, leaving essentially no room to improvise an escalation process after the fact [7]. Organizations that treat vulnerability triage as a periodic or batched activity, rather than a continuously staffed function with clear ownership, are unlikely to be able to meet a 24-hour early-warning deadline.

CSA's prior survey work on SME CRA readiness suggests the scope question is where organizations are most likely to be caught off guard: the reporting duty attaches to the product, not to whether the manufacturer considers the product under active development, and it applies to products already on the EU market before the CRA's full application date — meaning legacy and end-of-primary-development products are squarely in scope if they remain commercially available [5]. CSA's earlier analysis of ENISA's SME Cyber Resilience Maturity Assessment Model found that awareness of the CRA substantially

outpaced operational readiness among smaller manufacturers, with incident response and product lifecycle management identified as the weakest of the model's five assessed domains, particularly among microenterprises [5]. A manufacturer that can name the CRA and knows a deadline exists is not the same as a manufacturer with a staffed, tested process capable of filing a compliant early warning inside a day.

The SRP also introduces new identity and access-management surface area that security teams need to plan for administratively, not just technically. Access requires an EU Login account with multi-factor authentication, and each manufacturer designates a Primary Assigned Representative who manages the account relationship with the coordinating CSIRT and can invite up to twenty Secondary Assigned Representatives to submit and manage notifications on the manufacturer's behalf [8]. The platform allows a limited number of notifications before stricter identity verification is enforced, and it currently operates only in English, which is a practical friction point for manufacturers whose incident-response documentation and internal escalation language is not English-language by default [8]. None of this is exotic identity management, but it is one more system, with its own account-recovery and access-continuity requirements, that must be integrated into an organization's incident-response runbook before an incident — not during one.

Finally, the penalty structure gives the reporting obligation real enforcement weight rather than treating it as a procedural afterthought to the CRA's better-known secure-by-design requirements. Article 64 places non-compliance with Articles 13 and 14 — which include the vulnerability and incident reporting duty — in the CRA's highest fine tier, alongside breaches of the essential cybersecurity requirements themselves: up to €15 million or 2.5% of worldwide annual turnover, whichever is higher [6]. Providing false, incomplete, or misleading information to a notified body or market surveillance authority carries its own separate fine of up to €5 million or 1% of turnover [6]. The shared penalty tier suggests that reporting-duty violations are not treated as procedurally lesser than substantive security failures, though neither the CRA text nor ENISA guidance frames the tiering this explicitly. The table below summarizes the phased obligations manufacturers and open-source stewards are now operating against.

CRA Milestone	Effective Date	Applies To
Conformity assessment body registration begins	June 11, 2026	Notified bodies
Reporting obligations (24h/72h/14-day-or-1-month) via SRP	September 11, 2026	Manufacturers of products with digital elements

CRA Milestone	Effective Date	Applies To
Full essential cybersecurity requirements, CE marking, technical documentation	December 11, 2027	Manufacturers
Reporting obligations extend to open-source stewards	December 11, 2027	Open-source software stewards

Sources: [3][4][5][7]

Recommendations

Immediate Actions

Organizations that manufacture or distribute products with digital elements into the EU market should confirm, this week, whether they have designated a Primary Assigned Representative and registered for SRP access, since account setup and CSIRT-coordinator selection is a prerequisite that cannot be completed inside a live 24-hour reporting window [2][8]. Security teams should also audit whether their existing vulnerability-intake and incident-escalation processes actually name a single accountable owner for the "reasonable degree of certainty" determination that starts the CRA clock, rather than leaving that judgment ambiguous across security, legal, and product teams [7].

Short-Term Mitigations

Manufacturers should inventory legacy and end-of-life products still commercially available in the EU and explicitly confirm CRA reporting applicability for each, since the obligation is not limited to actively developed products [5]. Compliance and security teams should also build a single escalation runbook that reconciles CRA reporting timelines with parallel obligations under NIS2 and, where personal data is implicated, GDPR, since these regimes carry overlapping but not identical notification clocks and duplicating effort under time pressure increases the risk of a missed or inconsistent filing [7].

Strategic Considerations

Over the medium term, organizations should treat CRA reporting readiness as a standing operational capability rather than a one-time compliance project, given that open-source stewards face the same reporting duty from December 2027 and many manufacturers depend on open-source components whose upstream reporting behavior will affect downstream disclosure timelines [1][5]. Larger organizations that rely on smaller suppliers for CRA-regulated components should also incorporate CRA reporting-process maturity into third-party risk assessments, since CSA's prior analysis of ENISA's SME readiness data found that supplier immaturity in this area is a realistic source of inherited risk for the enterprises that depend on them [5].

CSA Resource Alignment

CSA's July 2026 analysis of ENISA's SME Maturity Model identified incident response and product lifecycle management as the weakest assessed domains — the same operational capacities the SRP's 24-hour clock now requires. ENISA's SME Maturity Model Exposes a CRA Readiness Gap analyzed ENISA's SME Cyber Resilience Maturity Assessment Model and a survey of 194 organizations across 31 countries, finding that incident response and product lifecycle management were consistently the weakest of the five assessed maturity domains [5]. That analysis's recommendation to establish a defined incident-escalation process ahead of the September 2026 deadline is now a binding operational requirement rather than a forward-looking suggestion.

The CRA's reporting windows do not operate in isolation: organizations already tracking mandatory patch-velocity timelines under other regimes, such as CISA's Known Exploited Vulnerabilities directives, should align internal service-level objectives to whichever applicable regulatory deadline is strictest, rather than to a median across jurisdictions. With the CRA's 24-hour early-warning window now legally live, that alignment is no longer a forward-looking recommendation but an immediate operational requirement for any organization selling covered products into the EU.

CSA's AI Controls Matrix (AICM) v1.1 provides the underlying control framework for operationalizing this work: its Threat and Vulnerability Management and Governance, Risk and Compliance domains map directly onto the intake, triage, and reporting-obligation-tracking processes the CRA now requires manufacturers to run continuously [9][5].

References

[1] European Union Agency for Cybersecurity. "The CRA Single Reporting Platform is launched." ENISA, September 11, 2026.

[2] European Union Agency for Cybersecurity. "Single Reporting Platform (SRP)." ENISA, 2026.

[3] European Commission. "Cyber Resilience Act - Reporting obligations." Shaping Europe's Digital Future, 2026.

[4] European Commission. "Cyber Resilience Act." Shaping Europe's Digital Future, 2026.

[5] Cloud Security Alliance. "ENISA's SME Maturity Model Exposes a CRA Readiness Gap." CSA, July 15, 2026.

[6] Official Journal of the European Union. "Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements." EUR-Lex, October 23, 2024.

[7] Freshfields. "Cyber Resilience Act reporting obligations take effect on 11 September 2026." Freshfields, September 2026.

[8] European Union Agency for Cybersecurity. "Single Reporting Platform (SRP) - Frequently Asked Questions." ENISA, 2026.

[9] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, July 2026.

