Nemko Digital



The CRA Reporting Clock Is Starting – Are You Operationally Ready?

> ***Why CRA reporting readiness is an enterprise capability—and how the internal escalation procedure enables it***

From 11 September 2026, CRA reporting becomes a live operational obligation. Manufacturers and open-source software stewards must report actively exploited vulnerabilities and severe incidents affecting products with digital elements through the Single Reporting Platform (SRP), beginning with an Early Warning within 24 hours of awareness and continuing through the 72-hour notification and final report. For business leaders, the exposure is broader than regulatory non-compliance: a missed or poorly governed submission can intensify customer concern, weaken confidence in product security, consume executive attention and compound the disruption of the underlying event. The decisive question is therefore not whether someone can access the ENISA submission portal, but whether the organisation can identify, assess, approve and evidence a regulatory decision while facts are incomplete and the clock is already running.

Consider a realistic test. A critical vulnerability is confirmed late on Friday before a long holiday weekend. Product security needs more evidence, legal wants a defensible interpretation, the product owner is travelling, and the Primary Assigned Representative (AR) is unavailable. Yet the CRA awareness clock does not wait for the next working day. The organisation must decide what is reportable, preserve the awareness timestamp, approve an accurate Early Warning and maintain a complete audit trail—without allowing uncertainty to become paralysis.

A credible reporting capability combines detection, product and market knowledge, legal interpretation, technical assessment, executive decision rights, evidence management, customer communication and continuous deadline control. The SRP is the reporting channel, and the AR is a key human control point within it; neither can compensate for unclear ownership, unavailable approvers, fragmented data or an untested incident process.

The Assigned Representative: a key enabler within the wider capability

ENISA's current user model places the Assigned Representative (AR) role at the centre of the manufacturer's interaction with the SRP. An AR authenticates through the EU Login portal, selects the CSIRT Designated as Coordinator, associates with a manufacturer or open-source software steward, and submits or updates notifications. Both Primary and Secondary/Backup AR users can participate in the reporting workflow, subject to their active status, role and association restrictions.

This makes the AR much more than a named account, but not the sole owner of CRA readiness. The role connects product security, incident response, legal, compliance, product management and the competent authorities. Its effectiveness depends on the surrounding governance: clear decision rights, accessible evidence, authorised approvers, continuity arrangements and a process that has been rehearsed under time pressure.

Role	Official SRP capability	Business implication
Primary AR	Registers through the main flow, associates with the manufacturer, can invite a Secondary AR, manage associations and perform notification activities.	Owns the operational reporting interface and should be supported by clear authority, escalation paths and evidence access.
Secondary/Backup AR	Registers through an invitation from the Primary AR and becomes associated with the relevant manufacturer as a backup user.	Provides resilience for absence, time-zone coverage, surge events and deadline continuity.

The SRP guides the AR through an Early Warning, a 72-hour Notification and a Final Report. It can save drafts, identify missing mandatory data, display pending actions and support updates. But it cannot determine whether evidence is reliable, whether a product is affected, whether exploitation is active, whether an incident meets the CRA severity criteria, or who inside the business may accept the regulatory and reputational consequences of the decision. The most serious operational failure is therefore decision latency: the organisation cannot make, approve and document a defensible judgment before the applicable deadline.

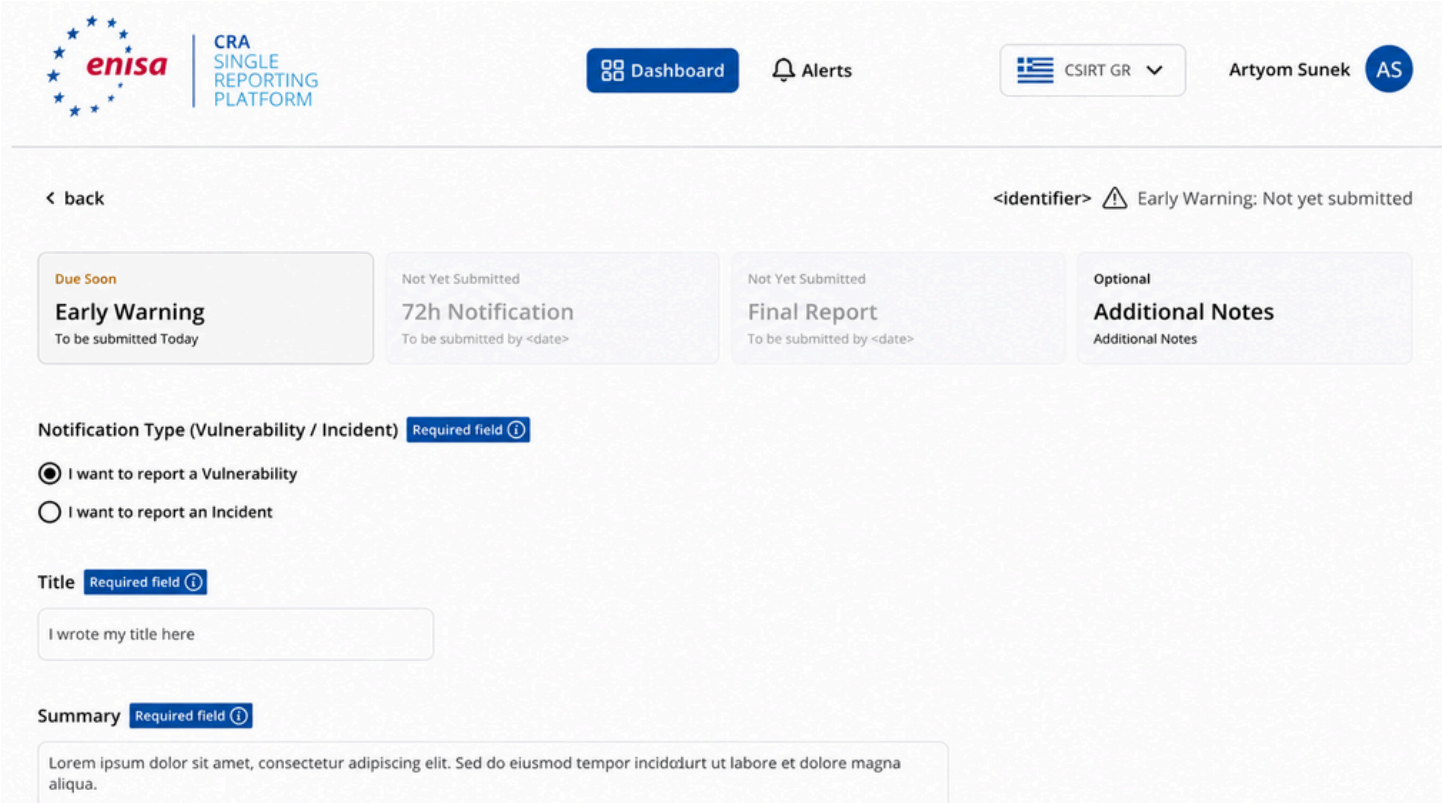


Figure 1: Early warning submissions page (Source: CRA SRP guidance - AR Notification submission and update | ENISA)

A mature capability begins before login. It needs a controlled intake, an auditable awareness timestamp, product and market mapping, technical evidence, pre-agreed decision criteria, rapid access to authorised approvers, deadline monitoring, customer-communication coordination and a tested fallback.

The AR orchestrates the SRP interaction, while the manufacturer remains responsible for reportability, factual accuracy, remediation and the broader business response.

What a high-performing CRA reporting operating model should deliver

- Authorised representation: a named Primary AR and tested Secondary AR, each using their own EU Login and operating under documented authority.
- Fast mobilisation: immediate access to product owners, security specialists, legal and compliance decision-makers.
- Evidence quality: structured capture of affected products, exploitation or incident evidence, impact, mitigation and corrective measures.
- Deadline control: explicit ownership of the 24-hour, 72-hour and final-report milestones, including receipt verification and follow-up.
- Continuity and auditability: backup coverage, controlled records, approval evidence and an outage or substitution playbook.
- Human accountability: automation may support completeness and consistency, but reportability judgments and submissions remain controlled human actions.

For manufacturers without a mature product security and regulatory incident capability, specialist support can reduce execution risk. Nemko Digital can help organisations assess CRA reporting readiness, review governance and decision rights, map product and evidence dependencies, run timed reporting simulations, strengthen incident-response readiness and provide managed compliance support during live cases. The commercial value is not “we submit a form for you”; t is helping the organisation make faster, better-evidenced decisions, protect continuity and demonstrate control when regulatory, customer and reputational pressure converge.

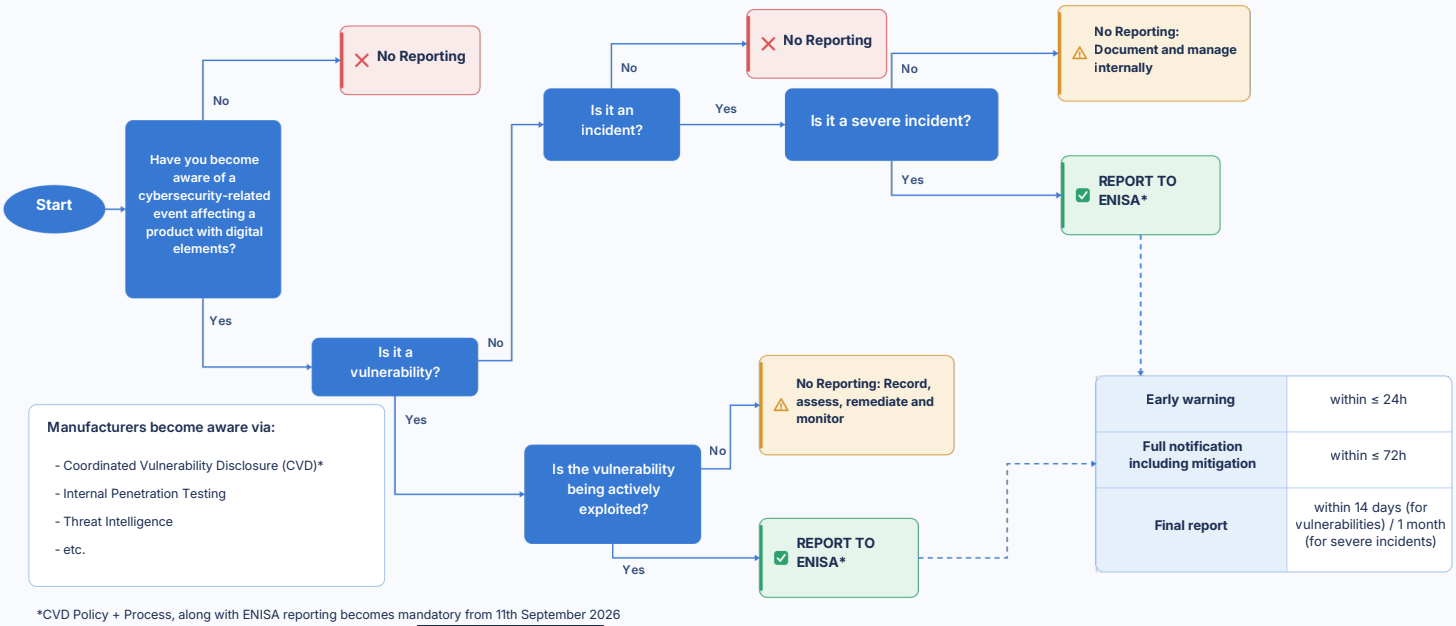
Would your organisation pass the 24-hour test?

Ask five questions:

- 1. Can we recognise a potentially reportable event and preserve the awareness timestamp at any hour?
- 2. Do named decision-makers have authority to determine, approve and document reportability within 24 hours?
- 3. Can we identify affected products, components, customers and Member States without assembling data from scratch?
- 4. Can either the Primary or Secondary AR access an approved evidence pack and submit when key personnel are unavailable?
- 5. Have we tested the complete process—including a Friday-evening or holiday-weekend scenario—and closed the gaps?

If any answer is uncertain, the organisation has a readiness gap.

CRA Article 14: Reporting Obligations



*CVD Policy + Process, along with ENISA reporting becomes mandatory from 11th September 2026

Executive takeaway

CRA reporting readiness is an enterprise capability, not a simple online portal submission task. The AR is an essential control point, but successful reporting depends on governance that can convert weak signals into timely decisions, mobilise the right experts, preserve evidence and maintain continuity under pressure. Organisations that prepare only the user account risk discovering that the real bottleneck is elsewhere. Organisations that rehearse the complete capability are better positioned to meet regulatory deadlines, protect customer trust and respond credibly when a product-security event becomes a board-level issue.

> **Recommended action:** Contact Nemko Digital to benchmark your CRA reporting capability through a readiness assessment, governance review and timed simulation—and to design the incident-response, evidence and managed compliance support needed before (and after) 11 September 2026.

About the author



Gustavo Sánchez

Gustavo brings strong expertise at the intersection of AI security, trustworthy AI, and assurance for high-stakes systems. With a research-driven mindset and hands-on experience tackling real-world challenges — from adversarial ML to critical infrastructure contexts — Gustavo helps customers build AI systems that are not only innovative, but also secure, reliable, and demonstrably trustworthy.

Nemko Digital