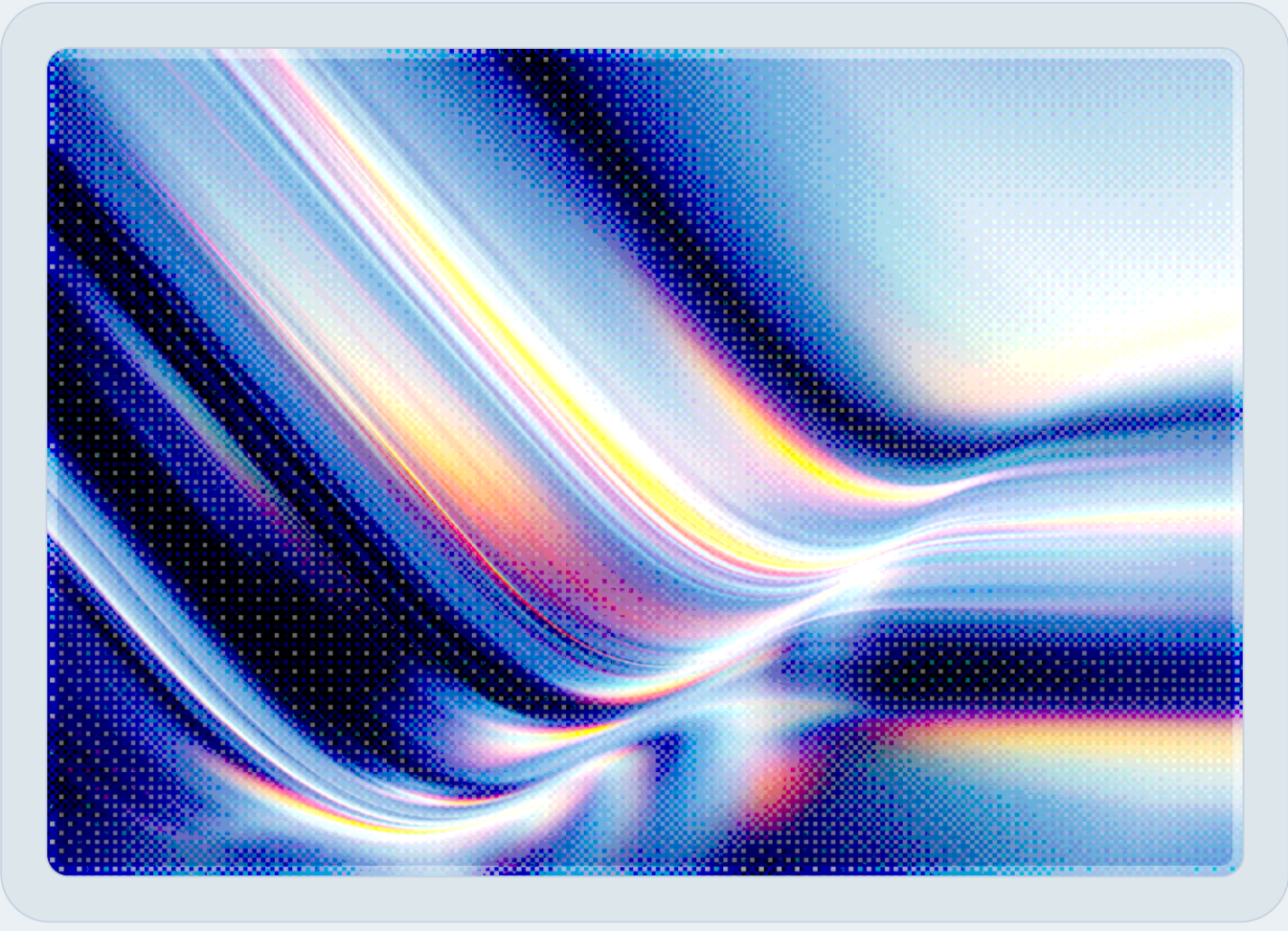
CSAI Foundation | Cloud Security Alliance

ENISA's SME Maturity Model Exposes a CRA Readiness Gap

2026-07-15

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

The European Union Agency for Cybersecurity published a new SME Cyber Resilience Maturity Assessment Model on July 13, 2026, alongside survey data showing that most small and medium-sized manufacturers know the Cyber Resilience Act is coming but lack the documentation, staffing, and technical processes to meet it [1][2]. Of the 194 organizations ENISA surveyed across 31 countries between February and March 2026, roughly two-thirds had heard of the CRA, yet the agency found practical understanding of the regulation's requirements consistently lagging behind that awareness [3]. Company size proved to be the strongest predictor of readiness: medium-sized firms scored, on average, a full point higher than microenterprises across every one of the model's five assessment domains, with incident response and product lifecycle management emerging as the weakest areas overall, particularly for the smallest respondents [1][3]. The new model itself is a self-assessment instrument, not a compliance certification, and ENISA is explicit that even an "advanced" maturity score does not demonstrate legal compliance with the CRA [2]. For security leaders inside SMEs, and for larger organizations that depend on SME suppliers within CRA-regulated supply chains, the gap this data reveals is not a knowledge problem so much as an execution and resourcing problem, one that will become urgent as the regulation's phased deadlines arrive over the next eighteen months.

Background

The Cyber Resilience Act, formally Regulation (EU) 2024/2847, entered into force in December 2024 and introduces horizontal cybersecurity requirements for essentially all software and hardware products with digital elements placed on the EU market [4][5]. Unlike sector-specific rules that preceded it, the CRA applies broadly to manufacturers, importers, and distributors regardless of size, requiring that products be designed and maintained securely across their entire lifecycle rather than assessed once at launch. The regulation is being phased in on a staggered timeline rather than taking effect all at once, which matters for how organizations should be sequencing their preparation.

Reporting obligations under Article 14, which require manufacturers to notify ENISA and their national competent authority of actively exploited vulnerabilities and severe incidents within 24 hours of becoming aware of them, take effect on September 11, 2026 [4]. Provisions governing the notification of conformity assessment bodies apply from June 11, 2026 [4]. The regulation's substantive requirements, including the essential cybersecurity requirements, technical documentation obligations, conformity

assessment procedures, and CE marking, become fully applicable on December 11, 2027 [4][5]. That date is now less than eighteen months away, and it applies uniformly to manufacturers of any size, including the smallest software vendors and IoT hardware producers that make up a substantial share of the EU's digital product ecosystem.

ENISA's own framing of the problem is direct: because SMEs constitute the majority of manufacturers, importers, and distributors of products with digital elements in Europe, their ability to understand and implement the CRA will materially shape whether the regulation succeeds as intended [2]. Many of these organizations do not operate dedicated security teams, and cybersecurity responsibilities are frequently distributed across staff whose primary roles lie elsewhere, in engineering, operations, or general management [2]. This structural reality plausibly explains why the European Commission and ENISA developed practical tools tailored to smaller organizations rather than assuming that SMEs would adopt the same compliance infrastructure as large enterprises.

To quantify the gap before publishing guidance, ENISA ran a structured survey between February and March 2026, gathering responses from 194 organizations spanning 31 countries, including 25 EU member states [3]. The survey examined CRA awareness, understanding of practical requirements, existing cybersecurity practices, assignment of organizational responsibility, and anticipated implementation challenges. That survey, published separately as the SME CRA Survey Report on June 24, 2026, forms the evidentiary basis for the maturity model ENISA released a few weeks later [1][3].

Security Analysis

The maturity model itself is structured around five domains that ENISA maps to the CRA's expected practices: governance and documentation; risk management and security by design and by default; vulnerability and patch management; product lifecycle management; and awareness, competence, and skills [2]. Each domain contains five assessment criteria, and each criterion is scored on a five-point scale ranging from "not implemented" to "measured, monitored, and continuously improved." Domain scores are averaged from their underlying criteria, and the five domain averages are then averaged again to produce an overall maturity score, which organizations map to one of three profiles: basic (1.0–2.5), intermediate (2.6–3.9), or advanced (4.0–5.0) [2]. The table below summarizes what each domain covers and how it connects to specific CRA obligations.

Domain	What It Assesses	CRA Connection
Governance and documentation	Defined roles, management-approved policies, product-level security	Technical documentation obligations demonstrating how

Domain	What It Assesses	CRA Connection
	documentation, supplier expectations, management review	products meet essential cybersecurity requirements
Risk management and security by design/default	Consideration of product-specific risks, threat and misuse scenarios, third-party/supply chain dependencies, secure-by-default configuration	Essential requirement that products be designed to minimize known risks and attack surfaces
Vulnerability and patch management	Identifying and tracking vulnerabilities, using external advisories and public databases, prioritizing by risk, distributing updates, drawing up a software bill of materials	Vulnerability handling and update-provision obligations, including the SBOM requirement in Annex I
Product lifecycle management	Defining support periods, providing updates throughout the declared support window, communicating end-of-support timelines, planning secure retirement	Post-market obligation to maintain security for the declared support period, not just at launch
Awareness, competence, and skills	General product security awareness, role-specific training, sharing lessons learned, use of external security information	Underpins consistent execution of the other four domains, especially where dedicated security staff are absent

Two design choices in the model are worth flagging because they shape how the results should be read. First, ENISA built the vulnerability and patch management domain around the expectation that manufacturers will maintain a software bill of materials for software products placed on the market, describing the SBOM as a structured inventory of proprietary and open-source components that helps manufacturers understand their own composition and prioritize remediation by exposure and criticality [2]. SBOM generation and maintenance is a nontrivial engineering investment for organizations that have historically tracked dependencies informally, and it is likely to be one of the more resource-intensive items on any SME's CRA roadmap. Second, ENISA is careful to state that the model "does not distinguish between different product categories," even though the CRA itself sorts products into

default, important, and critical tiers with different conformity assessment procedures; organizations still need to determine which tier their products fall into before they can know exactly which obligations apply to them, something the self-check alone will not tell them [2].

The survey findings give the maturity model empirical weight rather than leaving it as an abstract framework. Sixty-six percent of the 194 surveyed organizations had heard of the CRA, but ENISA found that awareness consistently outpaced practical understanding of what the regulation actually requires organizations to do [1][3]. This pattern is not unique to the CRA: name recognition often spreads through industry press and vendor marketing before operational detail catches up, and in this analyst's view that gap is where compliance risk tends to concentrate. Company size, meanwhile, was the strongest predictor of maturity in the survey data, with medium-sized enterprises scoring approximately one full point higher than microenterprises across all five domains [1][3]. Given that the maturity bands span only 1.0 to 1.5 points each, a one-point gap is large enough to routinely separate a microenterprise's "basic" rating from a medium-sized peer's "intermediate" or "advanced" rating on the same criteria.

The survey also identified where the weakest practices concentrate: incident response and product lifecycle management stood out as the weakest area overall, and the effect was most pronounced among microcompanies [1]. This finding is consistent with what the maturity model's own domain descriptions would predict. Lifecycle management requires an organization to make and keep commitments about support periods and update delivery long after a product ships, which is difficult to sustain without the dedicated process ownership that larger organizations are more likely to have. When 142 of the 194 respondents cited a need for financial support to close their compliance gaps, and a separate question found more than 70 percent requesting practical templates for technical documentation and secure development, the message from the survey population is less about awareness and more about a lack of the tooling, templates, and budget needed to convert intent into documented, repeatable practice [1].

Recommendations

Immediate Actions

Organizations that manufacture, import, or distribute products with digital elements in the EU market, regardless of size, should run ENISA's self-check questionnaire now rather than waiting for the December 2027 deadline to approach. The self-check takes approximately two hours to complete and produces a domain-by-domain maturity score that identifies which of the five areas needs attention first [2]. Because vulnerability and patch management, and specifically SBOM readiness, is both a CRA

obligation and a documented weak spot in the survey data, organizations without an existing software inventory process should treat SBOM generation as one of the first concrete deliverables coming out of the self-check, rather than a documentation exercise to defer until closer to the compliance deadline.

Short-Term Mitigations

Before the September 11, 2026 reporting-obligation deadline arrives, organizations should confirm they have a defined internal process for detecting, escalating, and reporting actively exploited vulnerabilities and severe incidents within the CRA's 24-hour notification window, and should identify who within the organization is authorized to file that report to ENISA and the relevant national authority [4]. This is one of the earliest-binding CRA obligations and applies to products already on the market, including legacy products, so it cannot be deferred alongside the longer-dated 2027 requirements. Organizations should also determine, using the CRA's product classification criteria, whether their products fall into the default, important, or critical tiers, since this determines which conformity assessment procedures apply and the ENISA model deliberately does not make this determination for them [2].

Strategic Considerations

Over the medium term, SMEs should treat the ENISA maturity model as a planning instrument rather than a compliance artifact, using its five domains to build a phased improvement roadmap that prioritizes high-risk gaps, such as the absence of a vulnerability tracking process or unclear regulatory responsibility, ahead of lower-risk documentation cleanup. ENISA itself recommends repeating the self-check periodically, such as annually or after major product updates, to demonstrate continuous improvement rather than a one-time snapshot [2]. Larger enterprises that rely on SME suppliers for components, software, or connected products should also recognize that this maturity gap sits inside their own supply chains: a CRA-regulated product that incorporates an SME-supplied component inherits that supplier's vulnerability management and SBOM practices, making supplier maturity assessment a reasonable addition to existing third-party risk programs rather than a purely regulatory concern confined to the SME itself.

CSA Resource Alignment

CSA's own published guidance connects directly to several of the gaps this survey surfaces. The SBOM and supply-chain dependency practices at the center of ENISA's vulnerability and patch management domain touch on material covered in CSA's Software Transparency: Securing the Digital Supply Chain, which discusses SBOM and VEX adoption alongside broader supply-chain incidents such as SolarWinds

and Log4j; SMEs building their first SBOM process as part of CRA preparation can use it as background context before moving to more implementation-specific tooling and templates. Because the survey's weakest respondents are concentrated among manufacturers of connected products, and product lifecycle management is one of the two domains ENISA identified as weakest overall, CSA's Forward Thinking Cybersecurity Manufacturing Best Practices and Roadmap to 2026 offers sector-specific guidance on the IT/OT/IoT security practices and regulatory alignment that overlap substantially with the CRA's product-security expectations for manufacturers, while CSA's Future Proofing the Connected World lays out concrete steps for securing IoT products across the development lifecycle, speaking directly to the lifecycle-management gap the survey identifies. For organizations that want to benchmark their ENISA self-check results against a broader security-program maturity lens, CSA's Measuring the Maturity of Your Cloud Security Program introduces the Cloud Security Maturity Model (CSMM), a comparable staged-maturity approach that can help SMEs whose products depend on cloud infrastructure extend the ENISA assessment beyond product security into the surrounding operating environment. Where organizations are building governance and risk-management processes with an eye toward AI-enabled products specifically, CSA's AI Controls Matrix (AICM) v1.1, with 247 control objectives spanning 18 domains, offers considerably more granularity in governance and risk than the ENISA model's single governance criterion, making it a useful reference for SMEs whose CRA-regulated products also incorporate AI components.

References

[1] ENISA. "Where do SMEs stand in preparing for the Cyber Resilience Act?" ENISA News, July 13, 2026.

[2] ENISA. "SME Cyber Resilience Maturity Assessment Model." European Union Agency for Cybersecurity, July 2026.

[3] ENISA. "SME CRA Survey Report." European Union Agency for Cybersecurity, June 24, 2026.

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

[5] Official Journal of the European Union. "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)." OJ L, 2024/2847, November 20, 2024.