CRA Presumption of Conformity: What It Means and Why IEC 62443 Is the Right Implementation Path

The EU Cyber Resilience Act tells manufacturers what they must achieve. It does not tell them how.

Annex I sets out the essential cybersecurity requirements. Products must be designed and developed securely. Vulnerabilities must be handled systematically. Updates must be delivered. Personal data must be protected. The obligations are clear in principle. What remains open is the question every product security team eventually arrives at: what gives us the most defensible path to demonstrating we actually meet them?

The CRA's answer is presumption of conformity. It is worth understanding precisely, because it is frequently misread in both directions, either overstated as a compliance shortcut, or dismissed as irrelevant until harmonized standards exist. Neither reading is accurate.

What Presumption of Conformity Actually Means

The CRA, like most EU product regulation, operates on a presumption mechanism tied to harmonized standards. When a manufacturer implements a harmonized standard that has been formally published in the Official Journal of the EU, and that standard covers the relevant essential requirements, the manufacturer is presumed to be in conformity with those requirements.

The practical effect is a shift in the burden of proof. Without a harmonized standard, a manufacturer must construct an independent case for how each Annex I requirement is met, from first principles, in a form that holds up under conformity assessment. With a harmonized standard, that work has already been done at the standard's level. Implementing the standard is itself the evidence.

One important clarification: presumption of conformity is not a guarantee of compliance. A manufacturer can implement a harmonized standard and still fall short of Annex I if the actual practice doesn't match documented processes, or if the standard doesn't cover a particular requirement. The presumption shifts the burden. It does not eliminate the need for genuine implementation.

The standard does the evidentiary work. You do the implementation.

How Conformity Assessment Works in Practice

Understanding what presumption of conformity delivers requires understanding what a conformity assessment actually involves.

Most products will follow self-assessment under Module A of the CRA. The manufacturer conducts its own assessment, compiles a technical file demonstrating how the product meets Annex I requirements, issues an EU Declaration of Conformity, and applies CE marking. No external auditor is involved. But "self-assessment" does not mean unchecked. Market surveillance authorities can request the technical file at any point, and that file needs to hold up under scrutiny.

Products listed in Annex III require mandatory third-party assessment by a notified body. These are the higher-risk critical product categories, e.g. firewalls, VPNs, routers, SIEMs, and others. For these, a notified body reviews the technical documentation, assesses the conformity evidence, and issues a certificate. Notified bodies apply their own rigor, and capacity is already constrained as the December 2027 deadline approaches.

In both cases, the core challenge is the same: producing credible, traceable evidence that security was engineered into the product and maintained across its lifecycle. A recognized standard provides the structure that makes that evidence coherent rather than ad hoc.

Self-assessment is not a free pass. It is an unsupervised exam with open-book results.

The Current Gap: No Formally Designated Harmonized Standards Yet

Here is where the practical picture becomes important to understand clearly.

On 3 February 2025, the European Commission officially issued Standardization Request M/606 to CEN, CENELEC, and ETSI. The request was accepted in April 2025. The work is structured across four standard types: horizontal framework standards, vulnerability handling standards, technical measures standards, and product-category-specific vertical standards for Annex III product categories.

Current planning targets publication between August and October 2026 for the first deliverables, with the full set expected by October 2027, shortly before the CRA enters full application. The work is active and progressing on a defined standardization track. But no harmonized standards have yet been formally published in the Official Journal under the CRA.

This means the presumption of conformity mechanism is currently available in principle and unavailable in practice. Manufacturers implementing IEC 62443 today cannot formally invoke it. That matters for how the current investment should be understood, but it does not change the strategic calculation, as the next sections explain.

The mechanism exists. The standards to invoke it do not yet.

Why IEC 62443 Is the Right Path Anyway

IEC 62443 is widely expected to form the backbone of the harmonized standards that will eventually enable presumption of conformity for industrial and connected products. This expectation is grounded in the current standardization direction. The CEN-CENELEC standardization work is explicitly built on adapting the 62443 series into harmonized European

standards. The European Commission's direction to standards organizations names 62443 as a foundational reference. The ECSO survey on CRA challenges found 62443 to be the most frequently cited existing standard by manufacturers preparing for compliance.

The reason is structural: IEC 62443 is not a high-level governance framework. It translates directly into development practice, in a way that maps closely to what the CRA's Annex I requires.

IEC 62443-4-1 defines a secure development lifecycle, including structured practices for security requirements management, threat and risk analysis, secure design, implementation guidance, verification activities, and vulnerability management. This maps to the CRA's core expectations for how products are developed: security is not added at the end, it is engineered throughout.

The CRA's vulnerability handling obligations, covering coordinated disclosure processes, patch delivery timelines, and the need for systematic intake and triage, map to the vulnerability management practice group in 62443-4-1. The standard requires documented processes for tracking and remediating vulnerabilities across the product lifecycle, including defined processes for working with external researchers, which directly aligns with what the CRA expects.

IEC 62443-4-2 defines technical security requirements at the component level: authentication controls, communication integrity and confidentiality, protection against unauthorized access, and requirements for update integrity verification. These map to the CRA's product-level security requirements in Annex I, part I, which specify that products must resist unauthorized access, protect data in transit and at rest, and deliver authenticated updates.

This overlap is substantial. For organizations that have already implemented 62443, the CRA does not require starting over. It requires extending and adapting.

IEC 62443 doesn't describe security. It engineers it.

Where IEC 62443 Currently Falls Short

Stating the overlap accurately requires stating the gaps equally accurately. There are four areas where the current 62443 standard does not fully cover CRA obligations, and where manufacturers need to build separate compliance tracks.

SBOM provision

The CRA requires manufacturers to identify and manage software components and dependencies across the product lifecycle. In practice, this makes SBOM generation the most viable

implementation approach. For many products, that means maintaining a machine-readable inventory of components, including third-party software. IEC 62443-4-1 addresses supply chain security in principle and recommends practices for managing third-party components, but it does not mandate structured SBOM generation and disclosure as a required product deliverable. For many industrial product organizations, this represents the largest practical implementation gap.

Mandatory reporting timelines

The CRA requires manufacturers to report actively exploited vulnerabilities or severe incidents to ENISA within 24 hours of becoming aware of them, with a follow-up report within 72 hours. This specific regulatory notification obligation has no direct counterpart in 62443-4-1. The standard addresses internal vulnerability management process maturity, but it does not define legally bound external reporting timelines to regulatory authorities. These are fundamentally different obligations, and the reporting infrastructure required to meet them needs to be built independently.

End-of-support declarations

The CRA requires manufacturers to define and communicate a minimum security support period for each product, to deliver security updates throughout that period, and to notify users explicitly when the support period ends. IEC 62443 addresses lifecycle security in a general sense, but it does not require this kind of formal, market-facing commitment as a compliance deliverable.

Privacy and data protection

CRA Annex I requires that products minimize the processing of personal data, protect personal data by default, and prevent unauthorized access to personal data stored or transmitted by the product.

IEC 62443 was not designed for that problem space. Its confidentiality requirements are rooted in industrial operations, not GDPR-style privacy engineering. For products that handle personal data, this creates a separate compliance track that 62443 alone does not cover.

Knowing where a standard ends is as important as knowing where it begins.

What the EN Adaptation Is Doing to Close These Gaps

The standardization work currently underway is explicitly designed to adapt the 62443 series into harmonized European standards that address CRA requirements, including the gaps identified above. Two amendments are in active development.

EN IEC 62443-4-2:2019/A11:2026 is the primary vehicle on the technical side. The amendment work includes adapting existing component requirements to the CRA framework and introducing targeted enhancements to close identified Annex I gaps. It also defines applicability criteria, aligns the evaluation approach with expected conformity assessment artefacts, and specifies Security Level-based acceptance criteria for each requirement. This last point connects directly to the Applicability Assessment Requirements approach introduced in prAA, which shifts the framework from declaring a security level to individually justifying each requirement decision. The planned publication target for this amendment is October 2026.

EN IEC 62443-4-1:2018/A11:2026 runs in parallel on the lifecycle side. This amendment adds requirements around documenting intended use and security context, and further specifies the expected development artefacts that demonstrate a compliant lifecycle process has been followed. This directly addresses the CRA's demand for traceable evidence that the product was designed securely from the start, rather than asserted after the fact.

In addition, six vertical standards are planned for specific Annex III product categories, including VPNs, routers, SIEMs, and firewalls. These will provide product-specific technical guidance where the horizontal amendments leave room for interpretation, and are expected by October 2026.

One important caveat: the amendment work is clearly directional, and the scope is explicitly aligned with closing CRA gaps. But the degree to which the published amendments will fully address the SBOM, mandatory reporting, end-of-support, and privacy gaps in their final form remains to be confirmed once the text is published. The privacy gap in particular sits outside the natural scope of what a 62443-derived standard would address, and manufacturers should not assume it will be covered.

The direction is clear. The completeness is not yet confirmed.

What Manufacturers Should Do Now

Three actions follow directly from this analysis.

1. Implement IEC 62443-4-1 and 4-2 now.

Not because harmonization is confirmed, but because it structures your evidence base in a way that will carry formal presumption weight once the standards are designated, and already provides the most credible and auditable compliance path available today. Organizations that have already implemented will be positioned to transition to a presumption-of-conformity position quickly. Those who wait will not.

2. Address the four gaps as dedicated workstreams

SBOM infrastructure, ENISA reporting processes, end-of-support policy documentation, and privacy engineering are not optional CRA obligations that harmonization will eventually solve for you. They need dedicated implementation now, regardless of where the EN adaptation lands. Build them alongside your 62443 work, not after it.

3. Explicitly map IEC 62443 implementation to CRA Annex I

Do not assume auditors or notified bodies will connect the dots. For each Annex I requirement your 62443 implementation addresses, document how, with traceable references to your actual processes and artefacts. When the EN amendments are formally designated, converting your existing evidence base to a presumption-of-conformity position should be a documentation update, not a technical re-assessment.

Waiting for certainty is a decision. It just isn't a good one.

Closing

Presumption of conformity is not a compliance shortcut. It is a legal mechanism that rewards manufacturers who invested in structured, standards-based implementation before the regulatory deadline arrived.

The harmonization work is active and progressing in the right direction. The gaps are known and being addressed. Organizations that read the current absence of formally designated standards as a reason to wait are misreading the situation.

The gap between where harmonization stands today and where it will be when the CRA enters full application in December 2027 is not a window of uncertainty. It is a window that is closing.

Presumption of conformity is not a shortcut for those who waited.
It rewards early structure.

About the author

Frank Leitner is a product security specialist focused on Secure-by-Design development practices, structured threat modeling, and the implementation of ISA/IEC 62443 in software-driven and connected products.

He supports organizations in embedding security into their development lifecycle and translating regulatory expectations, such as those introduced by the EU Cyber Resilience Act, into structured engineering processes, traceable requirements, and verifiable technical capabilities.

His work centers on aligning security architecture, product management, and engineering disciplines to enable sustainable, compliance-ready product development.

Website: https://www.frank-leitner.com

#CyberResilienceAct #ProductSecurity #IEC62443 #SecureByDesign #SoftwareSecurity